UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

21839 7590 03/11/2005

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
TRAN, TONGOC	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/11/2005

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/586,977	06/05/2000	Bruno Basquin	032326-031	8497

TITLE OF INVENTION: PRE-CONTROL OF A PROGRAM IN AN ADDITIONAL CHIP CARD OF A TERMINAL

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$0	$1400	06/13/2005

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE REFLECTS A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE APPLIED IN THIS APPLICATION. THE PTOL-85B (OR AN EQUIVALENT) MUST BE RETURNED WITHIN THIS PERIOD EVEN IF NO FEE IS DUE OR THE APPLICATION WILL BE REGARDED AS ABANDONED.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL should be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). Even if the fee(s) have already been paid, Part B - Fee(s) Transmittal should be completed and returned. If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 12/04) Approved for use through 04/30/2007.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

or Fax **(703) 746-4000**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

21839 7590 03/11/2005

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (703) 746-4000, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/586,977	06/05/2000	Bruno Basquin	032326-031	8497

TITLE OF INVENTION: PRE-CONTROL OF A PROGRAM IN AN ADDITIONAL CHIP CARD OF A TERMINAL

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$0	$1400	06/13/2005

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRAN, TONGOC	2134	713-169000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____ 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are enclosed:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s):

☐ A check in the amount of the fee(s) is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

The Director of the USPTO is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.
NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/586,977	06/05/2000	Bruno Basquin	032326-031	8497

21839 7590 03/11/2005

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/11/2005

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 709 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 709 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571) 272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (703) 305-8283.

PTOL-85 (Rev. 12/04) Approved for use through 04/30/2007.

Notice of Allowability	Application No.	Applicant(s)	
	09/586,977	BASQUIN, BRUNO	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/14/2004*.

2. ☒ The allowed claim(s) is/are *1 and 3-19*.

3. ☒ The drawings filed on *16 September 2004* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2130

Notice of References Cited	Application/Control No. 09/586,977	Applicant(s)/Patent Under Reexamination BASQUIN, BRUNO	
	Examiner Tongoc Tran	Art Unit 2134	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	EP 292248	11-1988	European	Steiner	G07F 7/10
	O	DE 19523466	06-1995	Germany	Loehmann	H04L 9/32
	P	JP 9265516	10-1997	Japanese	Nishioka	G06K 17/00
	Q	EP 0858046 A2	12-1998	European	Copeland et al.	G06K 7/00
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	"Smart Cards: Java Gets Pats on Back From Card Business in Belgium and France", American Banker, v 164, n 61, p 16, March 31, 1999.
	V	Do, A. "Of Elvis and Smart Card Sightings", Automatic I.D. News, May 1997, Vol. 13 Issue 6, pS.20, 2p, 1c.
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

11/5,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00945654
Method and apparatus for integrated circuit card
Verfahren und Gerat fur eine Chipkarte
Methode et appareil pour une carte a puce
PATENT ASSIGNEE:
INFO TELECOM, (1418712), Rue de la Foret, B.P. 9, F-67550 Vendenheim, (FR), (Applicant designated States: all)
INVENTOR:
Copeland, Jeffrey P., 358 Quinapoxet Street,, Jefferson, Massachusetts 05122, (US)
Vandenengel, Gerald W., 27 Millbury Street, Grafton, Massachusetts 01519, (US)
Chau, Paul W., 26 Travis Road, Natick, Massachusetts 01760, (US)
LEGAL REPRESENTATIVE:
Casalonga, Axel et al (14511), BUREAU D.A. CASALONGA - JOSSE Morassistrasse 8, 80469 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 858046 A2 980812 (Basic)
EP 858046 A3 990908
APPLICATION (CC, No, Date): EP 98300877 980206;
PRIORITY (CC, No, Date): US 37696 P 970207
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06K-007/00

ABSTRACT EP 858046 A2
A portable integrated circuit card reader system provides for enhanced functionality and interconnectability with external devices. A printed circuit board arrangement includes a housing having first and second parallel planar surfaces and a printed circuit board disposed in the housing, including a substrate having a thickness of about 0.020 in. (0.5mm), and including a portion which engages an external connector through an opening in the housing. The printed circuit board is held by the housing at a first position, parallel to and between the planar surfaces of the housing, at the opening in the housing, and is held at a second position different from the first position, parallel to the planar surfaces of the housing and adjacent to the first parallel planar surface of the housing, the printed circuit board having a flex region between the first position and the second position. An interface module includes a housing, serial transceiver circuitry disposed in the housing, a first input/output connector which connects to an input/output port of the portable IC card reader, a cable coupling the connector to the transceiver circuitry, and a second input/output port which couples the serial interface module transceiver to an external device. A method of operating the portable IC card reading device includes reading a stored value from an IC card when the IC card is inserted in the device, receiving user input corresponding to an amount of a planned purchase, and automatically calculating and displaying an expected balance after the planned purchase. Further, after making the planned purchase with the IC card, a stored value from the IC card is read when the IC card is inserted in the device, and the value read is displayed.
ABSTRACT WORD COUNT: 282
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Withdrawal:	001129 A2	Date application deemed withdrawn: 20000309
Application:	980812 A2	Published application (Alwith Search Report ;A2without Search Report)
*Assignee:	981028 A2	Applicant (transfer of rights) (change): INFO TELECOM (1418712) Rue de la Foret, B.P. 9 F-67550 Vendenheim (FR) (applicant designated states:

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 858 046 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.08.1998 Bulletin 1998/33

(51) Int. Cl.[6]: G06K 7/00

(21) Application number: 98300877.2

(22) Date of filing: 06.02.1998

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 07.02.1997 US 37696 P

(71) Applicant: OKI AMERICA, INC.
Hackensack, NJ 07601 (US)

(72) Inventors:
- Copeland, Jeffrey P.
Jefferson, Massachusetts 05122 (US)
- Vandenengel, Gerald W.
Grafton, Massachusetts 01519 (US)
- Chau, Paul W.
Natick, Massachusetts 01760 (US)

(74) Representative:
Read, Matthew Charles et al
Venner Shipley & Co.
20 Little Britain
London EC1A 7DH (GB)

(54) Method and apparatus for integrated circuit card

(57) A portable integrated circuit card reader system provides for enhanced functionality and interconnectability with external devices. A printed circuit board arrangement includes a housing having first and second parallel planar surfaces and a printed circuit board disposed in the housing, including a substrate having a thickness of about 0.020 in. (0.5mm), and including a portion which engages an external connector through an opening in the housing. The printed circuit board is held by the housing at a first position, parallel to and between the planar surfaces of the housing, at the opening in the housing, and is held at a second position different from the first position, parallel to the planar surfaces of the housing and adjacent to the first parallel planar surface of the housing, the printed circuit board having a flex region between the first position and the second position. An interface module includes a housing, serial transceiver circuitry disposed in the housing, a first input/output connector which connects to an input/output port of the portable IC card reader, a cable coupling the connector to the transceiver circuitry, and a second input/output port which couples the serial interface module transceiver to an external device. A method of operating the portable IC card reading device includes reading a stored value from an IC card when the IC card is inserted in the device, receiving user input corresponding to an amount of a planned purchase, and automatically calculating and displaying an expected balance after the planned purchase. Further, after making the planned purchase with the IC card, a stored value from the IC card is read when the IC card is inserted in the device, and the value read is displayed.

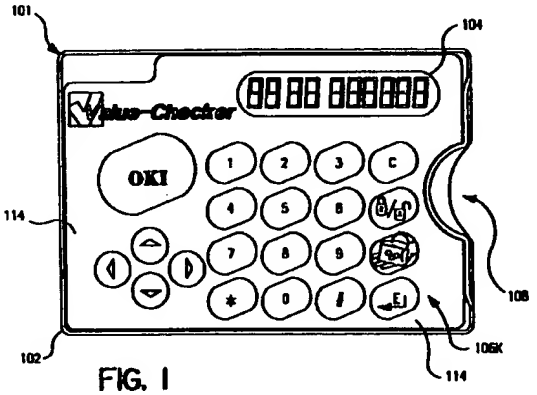


FIG. 1

EP 0 858 046 A2

Description

Field of the Invention

The invention relates to the field of integrated circuit (IC) cards (also referred to sometimes as "chip cards"), and in particular to IC card readers.

Background of the Invention

A so-called integrated circuit card, also referred to as a "smart card" and/or an "IC card" herein, is a credit card-sized carrier substrate, generally formed of a plastic material, which carries circuitry for storing information, such as financial information. These cards are gaining acceptance with many consumers as an alternative to cash for purchases. Smart cards can already be used in many countries of the world instead of coins or paper currency to make purchases. In a typical smart card electronic cash system, an IC on the card, either with an on-board micro-processor or just a memory chip, stores information, i.e., a "token," which represents the value or "balance" of electronic cash remaining on the card. As the user makes purchases with the card, this stored value is decreased electronically (internally) by the amount of the purchase.

Therefore, these IC cards are similar to a credit card with embedded integrated circuitry including, for example, both volatile and nonvolatile memory elements. The financial information is stored in these memory elements. In order to access the information in the IC card, an interface device, i.e., an IC card "reader," is required. There are two different kinds of IC card reader/interface systems classified based on their size and functionality. The first kind of IC card reader/interface device is referred to as a terminal device, e.g., a point of sale (POS) terminal, used for financial transactions. These device generally have a large size (form factor), but they have the capability to connect to other on-line systems, such as a financial institution, to provide a communication path between the IC card and the on-line systems. Due to their relatively large size, these terminals are mostly stationary and therefore cannot be carried around by the IC card user.

The second type of IC card reader/interface device is the portable IC card reader. Presently, these device are only used to provide static data display of the stored card information, and do not have the capability to connect to an on-line system to provide more sophisticated applications for the IC card.

There is also a variation of the first type of known IC card reader/interface device which is not as large as the usual terminal type, but is not as readily movable as the portable type. An example of this variation is described in Hirokawa (U.S. Patent 4,672,182). Such a device is designed to function with a personal computer as an add-on, but does not function as a stand alone unit, in contrast with the portable type device mentioned earlier. Such a device is, therefore, more like a terminal type device than a portable device, simply making the personal computer into an IC card terminal.

As should be clear from the above, the two basic kinds of reader/interface systems for IC cards offer either portability or connectivity, but not both. The terminal device is too large to be portable, and the portable device has limited functionality, lacking any communication ability, as compared with the terminal device. There is therefore a need for an IC card reader/interface system combining the benefits of both the terminal and portable type devices.

The portable type device have the advantage of being small enough to carry on one's person. However, the existing portable device does not provide very much functionality to the user, primarily merely providing the ability to view the value stored on the IC card. Additional functionality would be desirable, for example, when a POS terminal type device is not readily available.

In order to provide communications capabilities with external device, the data stored on the IC card must be converted to a form readily transmittable to external device, and reliability of the transmission must be assured. To meet this goal, there is a need for a programmed interface to implement the data conversion and transfer between the IC card and external device through a portable reader.

However, to provide communications capabilities for a portable type device, there are various technical hurdles to overcome. For example, interface circuitry must be compact yet provide sufficient communication ability, in order to provide the desirable functionality without sacrificing the small size of the typical portable device. In particular, interface connections must be designed so as not to unduly increase the thickness of the device which would make it unsuitable for carrying in a wallet, or shirt pocket, for example.

It should also be mentioned that there are a number of U. S. patents relating to various IC cards, card readers and related background technology, and some of these are now listed (alphabetically): Avery et al. (4,719,338); Bergeron (4,764,666); Broschard, III (5,599,203); Burkart (5,584,043); Dethloff et al. (4,968,873); Diehl et al. (5,128,523); Guion (4,675,516); Hara et al. (4,918,631); Harris Jr. et al. (Des. 323,489); Hirokawa (4,672,182); Huis et al. (5,550,361); Iijima (5,369,760); Iijima (5,581,708); Ishii et al. (5,541,985); Iwamoto et al. (Des. 370,213); Johnson et al. (5,149,945); Kapp et al. (5, 233,547); Koenck et al. (5,410,141); Kreft (5,619,683); Kumar (5,265,951); Kuwano et al. (4,922,111); Lei (5,373,146); Luong (Des. 348,439); Marceau et al. (5,491,326); Masuzawa et al. (5,015,830); Mori (4,877,947); Nitta (4,851,654); Oogita (5,227,615); Ozawa et al. (5,357,091); Parienti (5,189,287); Rey (5,272,319); Roberts et al. (5,438,184); Shino (5,296,692); Takahashi (5,406,064); Tatsuno (4,870,604); Terada et al. (5,561,628); Ugon et al. (4,523,297); Vandenengel (5,517,011); and Yoshi-

matsu et al. (5,615,388).

Further regarding functionality, while the electronic nature of the IC "cash" provides convenience, it also presents some problems or limitations for the user or owner of the card. In particular, there are limitations and problems associated with calculating the expected balance remaining on a smart card after a purchase. For example, when a consumer makes a normal purchase with a cash transaction using coins or paper currency, an amount greater or equal to the exact purchase price is given to the retailer, after which the retailer returns the appropriate amount of change, i.e., the difference between the purchase amount and the amount tendered. Upon receiving the change, the consumer can easily verify that the correct amount of change has been returned by counting with the change upwards starting from the purchase amount to the amount tendered, for example.

For example, a consumer makes a purchase for $12.73, and gives the merchant $15, using a ten dollar bill and a five dollar bill. The merchant returns $2.27 to the consumer, giving two one dollar bills, one quarter, and two pennies. The consumer verifies that this is the correct change amount by counting upwards with the change, for example: $12.73 plus $2 = $14.73; $14.73 plus 2 cents = $14.75; and $14.75 plus 25 cents = $15.00, the amount tendered.

This calculation is fairly easy to make as it does not require any subtraction with carry, for example, and can also be done step-by-step with the different currency units returned. In some simpler cases, the consumer may also elect to give the exact change, or the exact change for only the decimal part of the value. For example, on a purchase of $12.73, the consumer has the option, if he has the change available, of paying the exact amount of $12.73, or alternatively, paying the exact amount for the decimal portion, e.g., $15.73. In either of these cases the expected change calculation is simplified further or unnecessary.

However, when a purchase is made using electronic means, i.e., an IC card, calculating the expected change is considerably more difficult, while at the same time the requirement to do so is even stronger, since one could be short-changed without knowing it. While in a paper/coin transaction, the consumer typically only gives the retailer the lowest possible amount of money contained in his purse or wallet, in the case of smart card electronic transactions, the consumer is required to present the complete value contained within the IC card to the retailer. This clearly increases the risk of being short-changed by the retailer.

The calculations required to compute the expected change are made much more difficult in this case for at least the following reasons:

1. The amount or balance on the smart card will rarely be an integral number of currency units or contain the exact decimal value of the purchase. For instance, on the previous purchase of $12.73, the consumer may already have a balance of $16.22 on his or her card.

2. The consumer must calculate the expected balance on his or her card after the purchase by performing a subtraction of the purchase price from the balance previously on his or her card. In other words, it is not possible to count up from the purchase price since no change is physically returned. The transaction is essentially equivalent to the consumer giving his or her full wallet to the retailer, and relying on the retailer to remove the correct amount of money. In many cases, this subtraction will also require one or more carries, increasing the chances for error on the part of the consumer. For instance, on the purchase of $12.73 on a card containing $16.22, two carries are required due to the decimal amounts.

Therefore, there is a need for a way to allow the consumer to be able to easily determine the expected remaining balance on his or her IC card prior to and/or after an electronic cash purchase.

With the need for providing increased functionality, as described above, comes the need for a source of power adequate to provide the energy consumed by the associated electronics. IC card reader devices in the past had a sole source of energy, either from the internal batteries or an external means. These and other problems are addressed by various aspects of this invention relating to smart power management, which can manage several sources of energy simultaneously. When the reader is engaged with an external system, the internal batteries or an additional energy source can be activated when required for operation.

Summary of the Invention

It is an object of the invention to provide an enhanced portable IC card reader device.

It is a further object of the invention to provided a device which overcomes the problems mentioned above.

These and other objects of the present invention are accomplished by the method and apparatus disclosed herein.

An exemplary embodiment of the IC card reader according to the invention is advantageously provided with an input-output (I/O) port for connecting an external interface module to provide communication capability and functionality comparable to the terminal type reader. Further, the interface module can take a variety of forms, including RS232, infra-red (IR), radio frequency (RF) or a modem for interfacing with telephone lines.

The problems associated with interfacing with an external device without adversely affecting the device thickness, is solved according to one aspect of the

invention by flexing, or bending, the circuit board. In particular, the board I/O fingers are extended so the board is flexed without undue stress. Near the I/O connector, the board is held between two surfaces in the surrounding plastic case to hold it perpendicular to the outside wall.

An exemplary embodiment of the invention having a solution to the problem of determining the expected change in an electronic transaction by allowing the consumer to easily calculate the expected remaining balance on his or her smart card prior to a purchase. This invention proposes a simple solution to the problem of verifying the correct purchase amount and expected balance when using smart card electronic cash for purchases. It combines a card reader with a keypad in such a way that the user can quickly and accurately verify the expected balance on his or her card following a purchase.

An exemplary embodiment of the invention having a battery compartment for holding two batteries to provide the power necessary to operate the electronics associated with the increased functionality, is provided according to another aspect of the invention.

Brief Description of the Drawings

These and other features, aspects and advantages are provided by embodiments of the invention described below in the detailed description of the invention and illustrated in the accompanying drawings, in which:

Figs. 1 and 1A-1C illustrate the external appearance of the IC card reader/interface device according to an exemplary embodiment of the invention;

Fig. 2 is an exploded view of the exemplary device of Fig. 1, showing how an interface adapter plug would connect to the device and how batteries would be placed according to an exemplary embodiment of the invention;

Figs. 3 and 3A-3F illustrate a battery tray according to an exemplary embodiment of the invention;

Fig. 4A is a transparent view of the IC card reader device according to one exemplary embodiment of the invention, with an interface module connector connected thereto;

Fig. 4B is a side view of the device according to Fig 4A showing the connector channel;

Fig. 5 is a cross section showing how the circuit board of an exemplary embodiment of the device is bent and held in place;

Fig. 6 is an illustration of an exemplary embodiment of the device showing a pair of devices and interface modules, one with an interface module and connector in a connected condition, and one in an unconnected condition with the battery tray pulled out;

Fig. 7 illustrates the same arrangement as Fig. 6 except that the pair of devices are viewed from a different side, and the battery tray pulled out is not shown;

Figs. 8A and 8B illustrate an embodiment of the device and a basic block diagram of the exemplary embodiment, where the interface module has RS232 type transceiver circuitry;

Figs. 9A-9C illustrate an interface according to an exemplary embodiment of the invention, showing connector ends and the cable therebetween;

Fig. 10 is a state diagram of three operating modes and the transitions therebetween according to an exemplary embodiment of the invention;

Figs. 10A, 10B and 10C are portions of a flow chart of the operation of an exemplary embodiment of the invention;

Fig. 11 is a flow chart of the operation of an interface system according to an exemplary embodiment of the invention;

Fig. 12 is a block diagram of an exemplary embodiment of the invention having a PC interface unit;

Fig. 13 is a block diagram of an exemplary embodiment of the invention having an infra-red (IrDA) interface system;

Fig. 14 is a block diagram of an exemplary embodiment of the invention having a radio frequency (RF) interface system;

Fig. 15 is a block diagram of an exemplary embodiment of the invention having a modem interface unit;

Fig. 16 is a block diagram of an exemplary embodiment of the invention having a modular interface system, and showing the three layers of communication protocol;

Fig. 17 is a flow chart for a first exemplary embodiment of a change-checking method according to the invention;

Fig. 18 is a flow chart for a first alternate exemplary embodiment of a change-checking method according to the invention;

Fig. 19 is a flow chart for a second alternate exemplary embodiment of a change-checking method according to the invention;

Fig. 20 is a flow chart for a third alternate exemplary embodiment of a change-checking method according to the invention;

Fig. 21 is a schematic diagram for an exemplary embodiment of an interface system according to the invention; and

Fig. 22 is a schematic diagram of an exemplary embodiment of the invention.

Detailed Description of the Preferred Embodiments of the Invention

The invention will now be described in more detail by way of example with reference to the embodiments shown in the accompanying figures. It should be kept in mind that the following described embodiments are pre-

sented only by way of example, and should not be construed as limiting the inventive concept to any particular physical configuration.

An exemplary embodiment of the invention is illustrated in Fig. 1. An embodiment of the present invention in a commercial form is known as the ValueChecker-PLUS (VC+). This product is an enhancement over the original ValueChecker, incorporating enhanced capability and functionality (Value-Checker and ValueChecker-PLUS are proprietary trademarks and all rights are reserved). (ValueChecker+ will also be used herein for ValueCheckerPLUS.)

The portable reader device 101 (ValueChecker+) of Fig. 1 includes a case 102 made of plastic, for example, a display 104, and a keypad 106K. The keypad 106K is a keypad entry (module) to allow a user to select a variety of predefined functions for use with IC cards. As illustrated, there is a 4 by 5 matrix of numeric and function keys, including as one column of the matrix, four arrow keys. The illustrated embodiment uses a pinpad-sized keypad having a 4 by 5 matrix. However, the invention is not limited to this particular key arrangement, but may encompass other key arrangements within the scope of the invention defined in the claims. A battery tray 112 is provided along one side of the device. A face plate or cover 114 is provided and bears the trademark and company name in the illustration. A slot 108 with a finger cut-out is provided for insertion and removal of an IC card. As can be appreciated from Fig. 1, the device is not much larger in dimensions than an IC card itself, enabling it to be placed conveniently in a shirt pocket or wallet, for example, due to the ingenuity of the engineering and design. The placement of elements described is subject to variation within the spirit of the invention. The placement shown in Fig. 1 is for the purposes of illustration of an exemplary embodiment of the invention.

An interface connector channel 110 is illustrated as provided along one edge of the case 102. With an additional interface module, e.g., a personal computer adapter (PCA) which will be described in more detail later, the capability to interface an IC card with a personal computer (PC) through the portable reader device 101 is provided. The embodiments of the VC+ PCA described later herein, are of a similar size and shape (form factor) as those which could be used with the previous ValueChecker device.

As mentioned at the outset, the compact design of the VC+ portable reader device 101 is one factor that differentiates it from previously known IC card reader devices, e.g., desktop smart card readers and POS terminals, and gives it the advantageous portability. The advantageous slim design opens up a variety of useful application possibilities for the mobile world in which we live.

In the illustrated, exemplary preferred embodiment, the portable reader device 101 is generally rectangular and sized to fit comfortably into a standard shirt pocket or wallet. However, other shapes and sizes are possible within the spirit of the invention, so long as the benefits of compact size and convenience are maintained.

Besides providing an interface to the PC environment when operating with the PCA, the VC+ when operating in the standalone mode is also capable of providing selective information from the IC card to a user. An on-board key pad entry (module) enables the user to control the operation of the portable reader device 101.

Providing ample power for the increased functionality is another object of the invention. With reference to Figs. 2 and 3, for example, a battery tray 204 having space for two batteries 210 is illustrated. The battery tray 204 may be located on any of the edges of the case 102, and slides in and out for easy access by way of a finger slot. As illustrated, contacts 206 and 208 electrically connect the batteries 210 to the electronic circuitry of the portable reader device 101 (e.g., a painted circuit board PCB). A circuit board 106 has the keys of keypad 106K disposed thereon, along with the electronics required for operation, which will be described later, and thus forms a key pad entry module 106. The circuit board is connected to the display by a ribbon connector 202 in the illustrated embodiment.

Providing a compact, modular IC card (chip card) interface system is another object of the invention. As mentioned before, the two kinds of conventional reader/interface systems for IC cards offer either portability or connectivity, but not both. In this invention, a novel modular IC card interface system is described. The modular IC card interface system is not only small enough to be portable, but also versatile enough to be capable of communicating with other systems through different mediums (e.g., RF, IR and RS232). An embodiment of the system according to the invention includes essentially two parts. The first part is a portable reader device 101 (Fig. 1) with the key pad entry (module) 106, an LCD display (module) 104, and an interface connector channel 110 (port). The second part is the interface module(s) including connectors, circuitry and cabling, e.g., 600 (see Fig. 6).

Figs. 1, and 1A-1C illustrate the external appearance of the IC card portable reader device 101 according to an embodiment of the invention and Fig. 2 is an exploded view of the portable reader device 101 of Fig. 1, showing an interface adapter plug 218 which would connect to the portable reader device 101, and how batteries 210 would be placed according to an embodiment of the invention. Adapter plug 218 has an electrical plug 220 which couples with connections 222 on an extension of the circuit board, as illustrated. As will be described later in more detail, this portion of the circuit board is flexed to provide a more compact yet sturdy design.

Fig. 2 also illustrates a bottom cover 214, IC card channel cover 212, the main portion of the case 102 and the top cover plate 114 in an exploded fashion. Figs. 3,

and 3A-3F show the battery tray 204 and contacts 206, 208, enlarged and in more detail.

Fig. 4A shows the connection of the portable reader device 101 to the connector 218 in a transparent view. The connector 218 engages the extended portion of the circuit board as previously described, at the interface connector channel 110 (shown also in Fig. 4B). The flexing of the circuit board in this area is shown in the cross section of Fig. 5. By flexing, the length "L" of the flex portion of the board is reduced, making for a more compact overall design. Maintaining a reduced thickness of the hand held IC card reader is an object of the invention. For a hand held IC card reader, the form factor is important in ensuring the device is convenient and easy to carry. Optimizing size and weight are two of the many factors required to achieve these goals. One dimension may be more important to the convenience of a hand held device than another. In the case of the design of a hand held IC card reader according to the present invention, the thickness of the device is important to portability. A device of this size should be able to easily fit into a shirt pocket, wallet or a small purse, and the thickness dimension largely determines how easily it can be carried in a shirt pocket or a wallet, for example.

As already mentioned above, the IC card portable reader device 101 according to the invention is advantageously provided with an input-output (I/O) port for connecting to external device. It is common for circuit board edge contacts, or "fingers," to be used as an I/O connector to exit a computer or other electronic system enclosure, for example. However, generally, in these cases, size is not a driving factor, and therefore ample space for a mating connector is usually available, or the circuit board is positioned such that connecting cable thickness does not require a change in the height of the device enclosure.

In the case of the IC card portable reader device 101 according to the present invention, the printed circuit board is provided as a second layer of the device structure at the top, for example (see Fig. 2, an exploded view of one embodiment of the device). This permits using a low cost covering label as the faceplate or cover 114 to finish off the device and complete the membrane switch keypad 106K at the same time.

However, if the I/O connection fingers 222 were not somehow repositioned below the covering label 114, there would be a need to create a bump in the surrounding case 102, or to expose the connection fingers 222 themselves and cause the adapter plug 218 to protrude above the top of the portable reader device 101. This problem is solved according to one aspect of the invention by flexing, or bending, the circuit board as will be further described below, and is illustrated in Fig. 5.

Regarding the idea of bending a printed circuit board, it is only known to use this concept with flexible contacts which are in the form of a cable connecting, for example, internal electronic circuit boards in a device In the present case, a substrate thicker than such flexible contacts was needed for the external cable system to connect to, e.g., a printed circuit board thickness of about 0.020 in. (0.5mm). This thickness requirement caused two design problems which needed to be overcome and which could have resulted in a substantial increase in the thickness of the portable reader device 101.

The problem area was at the I/O adapter plug 218 and connector 220 which, when connected to the circuit board at connection fingers 222, would have protruded above the plane of the covering label 114. Conventional design practices would have simply increased the thickness in order to fit the requirements of the I/O adapter plug. However, keeping thickness minimized is an object of the invention. Therefore, in the present invention, a non-standard, counter-intuitive bending of the circuit board below the plane of the label 114 was used to keep the portable reader device 101 from getting any thicker. However, by doing this there were two design considerations which had to be taken into account:

1) the board could not be flexed beyond its elastic limit without becoming fatigued or snapping; and
2) the connector region of the board should ideally be perpendicular to the external wall of the surrounding device case or else the connector contact integrity could be compromised.

To deal with these problems and design considerations, the circuit board I/O connection fingers 222 were extended, e.g., approximately 10 mm in an exemplary embodiment, so that the circuit board could be safely flexed. Near the I/O connector region, the board is held firmly between two surfaces S1, S2 in the case 102 which holds it perpendicular to the outside wall of the portable reader device 101 (see Fig. 5).

In this design, there is a thin slot, e.g., about 6mm thick, which can be created by a slide or side action in tooling. This slot creates an upper and a lower surface S1, S2 to hold the flexed printed circuit board and (PCB) perpendicular to the outside edge of the portable reader device 101. To assemble the portable reader device 101, first the PCB I/O connection fingers 222 are inserted into this slot between surfaces S1 and S2. Then the PCB is held down against the top of the case 102 while screws, or a heat stake process, for example, secures the PCB into the case 102. The case features and the length of the PCB I/O connection fingers 222 will automatically align and position the fingers 222 at the correct location (see Figs. 2 and 5).

In Fig. 5, an arrangement of the flexed circuit board is illustrated in a cross-sectional view. The adapter plug 218 easily connects to the edge E of the circuit board through the slot provided, the edge of the circuit board being held perpendicular between surfaces S1, S2 of the device case 102. Where the circuit board is flexed over the portion of length L and then brought back to

parallel, the covering label 114 can be installed flush with the top of the case 102 to form the membrane switch keypad 106K

Figs. 6 and 7 show two different views of an interface module 600 and card portable reader device 101, in attached and unattached conditions. As can be seen, the module case 602 is coupled via cable 604 to the connector 218, previously described. The module case 602 is shown with knobs 606 which are used to attach the module case 602 to a standard interface socket (not shown) such as is provided on the back of a PC or modem, for example. Threaded tips 606A are for screwing into threaded sockets to secure a plug 702 on the module case 602 to the external device, e.g., PC or modem, in question.

Figs. 8A and 8B show an embodiment of the portable reader device 101 and a basic block diagram of an embodiment of the electronic system of the device 101, and an interface module case 802 having therein an RS232 type transceiver circuit. A cable 804 couples the module case 802 to a connector 818, which connects to the portable reader device 101 at the interface connector channel 110. In this way, a micro-controller unit (MCU) 806 of the portable reader device 101 is interfaced for input and output with an external device through an interface port 820 and circuitry in the module case 802. The MCU 806 is coupled to the display 104, to the keypad 106K, and to an interface port 808 to an IC card 810 which can be inserted into the portable reader device 101. The RS-232 transceiver circuitry in the module case 802 interfaces to an RS-232 port of a PC or modem, for example, through a standard connector.

Fig. 8B is the block diagram of a typical embodiment of the invention, i.e., a VC+ portable reader device 101 with a PCA interface system 802, 804, 818. A summary of the system is now presented. The MCU 806 of the portable reader device 101, in an exemplary preferred embodiment, has the following features and characteristics. The MCU 806 is, for example, an 8 bit micro-controller with an internal LCD driver circuit to support up to a 12-character LCD display (a total of 116 segments) 104, a keypad interface for a 4 by 5 keypad matrix, an interface port 820 for a cable system, and an interface port 808 for an IC-card 810. Other types of micro-controllers could be used as one skilled in the art would understand, as could different keypads, and displays, the above description of a typical embodiment being presented for purposes of example and explanation only.

A typical LCD display 104 in an exemplary embodiment has the following characteristics. Display 104 is, for example, a ten-character display (a 12 numeric 7 segments display), wherein 5 additional segments can be used for special icons. Display 104 operates on 5 volts, and has ratios of 1/3 bias and 1/4 duty cycle, for example.

A typical keypad 106K in an exemplary embodiment has, for example, 20 keys arranged in 4 by 5 matrix (10 keys for digits and 10 keys for other functions). Keypad 106K has, applied thereon, for example, a printed silver ink top label 114, and the key switches would typically be membrane switches disposed as a keypad matrix on the top surface of the circuit.

A typical IC card interface port 808 in a preferred embodiment is compatible with ISO-7816, for example, and uses an off-the-shelf IC card connector (not shown) with card-in detection. According to the invention, a modified ISO protocol format would typically be used. The communication between the circuitry module case 802 and the portable reader device 101 through a 4 pin interface PC port 820, is based on a custom protocol described herein. The data transfer is based on block transfer, i.e., a block of data is transferred from one end to the other end in alternate order. Differences between the present invention's protocol and the ISO-7816 standard protocol are now explained.

According to the present invention, a unique "VC+ Protocol Format" is used. In this protocol, each data block consists of, for example, a header byte, a length byte, and a duplication of the header byte. A series of information bytes of the size indicated by the value of the length byte, and finally a checksum byte, are provided. The header byte is used to specify a particular one of a plurality of functions. The VC+ portable reader device 101 according to the invention supports the following exemplary functions: receiving a command data sequence from an external source and passing it down to the IC card for execution; transmitting response data after execution of a command from the IC card to an external source; and receiving displayable data from an external source and the IC card. Of course, a keypad data request and response function, a communication status and error information request and response, as well as power management functions, are also provided.

The connected mode of operation of the device includes two methods of IC card data transfer: pass-through and non-pass-through. In pass-through, the portable reader device 101 serves as a conduit for the data to flow between the IC card and an external source. In the second transfer method, non-pass-through, the portable reader device 101 will intercept the command and response data, and perform some operations thereon, e.g., data validation and/or error handling, for example.

In the ISO-7816 protocol, each data block consists of, for example, a prologue (3 bytes long) that includes NAD (address) bytes, PCB (status) bytes and LEN (lengthy) bytes, an information data section (the size of which is specified by the value of the LEN byte), and an epilogue (1 or 2 bytes long) that is used as a checksum for the whole block. In this protocol, the NAD is used for addressing, and the PCB to show the status of the transfer. However, this protocol does not offer control of other hardware peripherals (e.g., LCD or keypad), so its

capability is limited.

The cable interface 818-820 in a preferred embodiment is a PCMCIA type low profile SMT receptacle, there being a direct connection to the printed circuit board through edge connector fingers 222, with a total of four interface pins needed: VCC, RX, TX, and GND.

The power system in a preferred embodiment uses, for example, two CR 2016 lithium coin cell batteries 210 for powering the internal circuitry. The batteries 210 are replaceable by the user through battery tray 204 which slides in and out. However, power can be supplied by an external PC when in the device is operating in the connected mode, in accordance with so-called smart power management.

The cable subsystem includes, in one preferred embodiment, RS-232 transceiver circuitry embedded, for example, in a module case 802 formed integrally with a cable, and provides for a data transfer rate at 4800 BAUD, for example. The interface also contains power circuitry to extract power from the RS-232 port of the external PC, for use by the portable reader device 101.

Figs. 9A-9C illustrate an exemplary embodiment of a cable subsystem, i.e., an interface module 600 according to an embodiment of the invention showing typical connector ends 702, 218 and cable 604 therebetween. The exemplary illustrated system uses as the electrical plug 220 a specified 4 pin Molex connector (220) to connect the interface port 820 thereby connecting the portable IC reader device 101 to the interface module case 602. Using the same interface port 820, the portable reader device 101 can connect to several different types of interface modules 600, as will be described later. Figs. 9A-9C therefore show just one example of the connectors and cable which could be used to implement an embodiment of the invention.

Depending on the communication medium used for hooking up the IC card interface system (reader and interface module) with an on-line network, for example, the circuitry in the interface module case 602 is designed to convert the digital information extracted from the IC card and provided by the portable reader device 101 into other kinds of signals, such as RF, IR or RS232 formats, and vice versa. For example, an RS-232 (PC) interface module when connected with the portable reader device 101, enables the IC card data to be transferred to a PC through the PC's RS-232 port, and data from the PC can be transferred back to the IC card as well.

Figs. 10 and 10A-10C relate to operation processes and will now be described in detail. There are three modes of operation for the modular IC card interface system. The three operational modes are standalone/passive, standalone/active and connected mode. Fig. 10 illustrates these three operating modes in the form of a state diagram, and Figs. 10A, 10B and 10C illustrate the operating mode transitions in flow chart form.

When the portable reader device 101 is not connected to other systems, i.e., an interface module is not engaged, the portable reader device 101 is in a standalone mode. Upon powering on the portable reader device 101, it is in the standalone/passive mode. The portable reader device 101 will fetch and display predefined data from an IC card inserted therein. After the data display is finished, or when the display of data is interrupted by detection of the pressing of a key press, the portable reader device 101 goes into the standalone/active mode. When in the active mode, a user can perform various functions on the IC card by using the keypad 106K on the portable reader device 101. For example, the user can lock or unlock the IC card.

When an interface module such as described above is engaged, the system goes into the connected mode, communication control being from an external system. In the case of using an RS-232 interface in module case 602, software running in the PC may take total control over the communication port.

Figure 10 shows the relative transitions of these operational modes of the system. In more detail, the three modes are explained as follows. In the first mode, the standalone/passive mode, the following applies: the external interface (PC) port and the keypad data entry module are not active in this mode. The portable reader device 101 provides static (pre-defined) data from the IC card on the LCD display 104, i.e., balance, and/or traces data from the "purse." This mode is activated when a power-on button of the portable reader device 101 is pressed. At this time, the portable reader device 101 will display the static data on the LCD display 104 sequentially until it reaches the end of the sequence. After reaching the end of the display sequence, the portable reader device 101 will time out in 2 seconds if no key entry is detected during that time.

In the second mode, the standalone/active mode, the following applies: the external interface (PC) port is not active. Upon power-on, the user can set the portable reader device 101 to the active mode by interrupting the display sequence of the static data by depressing any key on the keypad 106K. Once the portable reader device 101 is in the active mode, the IC card remains activated and, the LCD 104 displays messages to instruct the user to enter data. The user can select a particular function by pressing a function key on the portable reader device 101. The portable reader device 101 determines the status of the IC Card and performs the requested function. At the termination of a particular function, the portable reader device 101 goes back to the active mode and waits for another function request. When the keypad entry module is idle for more than 15 seconds, the portable reader device 101 powers down the IC card and times out.

In the third mode, referred to as the connected mode, the following applies: the external interface (PC) port is active, i.e., when the portable reader device 101 is connected to the serial port, e.g., RS-232 of a PC,

through an interface adapter module, it will be in the connected mode. Instructions and data will be coming in and out of the PC. Power to the portable reader device 101 may be supplied and controlled by the PC as well. Any time-out routine will be handled by the software in the PC. When the portable reader device 101 is in the connected mode, the IC card will be able to interact with a high level application program in the PC.

Exemplary applications of the portable reader device 101 in each of the three modes can be summarized as follows.

Standalone/Passive mode: display pre-defined data/information from the IC card, command sequence and display procedure are masked in the MCU, self-start operation upon device power-on, real-time clock (Optional).

Standalone/Active mode: the user can select specified data display from the IC card by making the selection through the keypad, IC card locking and unlocking by means of the pin presentation, check-change/change-checker functions (described in more detail later), IC card data record updating, external data transfer into the card, and optional on-board calculation functions.

Connected mode: complex applications designed at a high level are translated into command stream and sent through the RS-232 port to the IC card, responses from the command executions are returned through the same path, customized communication protocol provides an integrated application environment which utilizes both the LCD and keypad control of the reader, and enables the PC to perform home banking applications with the IC card.

Fig. 11 is a high-level process flow chart for an embodiment of the invention utilizing the PC interface system. As illustrated in the process flowchart, a high level program for the interface system would operate in the following manner. At startup, the program initializes the serial port in the PC and establishes a communication link through the interface adapter and provides power to turn on the portable reader device. This also sets up the operation mode for the portable reader device. After initialization, the program will perform a classic command fetch and execute loop. The program will fetch a command or control data from the user, either by using an internal command sequence or an external command sequence entered through the keyboard. The program builds and sends out a data block that conforms to the custom protocol for the device, described above, to the portable reader device 101. The original command data embedded inside this data block will be extracted and processed by the micro-controller 806 in the portable reader device 101. If the command data is destined for the IC card, the portable reader device 101 will send out the command data to the IC card 810 through the card interface port 808. It then waits for the response generated by the command execution. For a data block that contains process control data, LCD output data, and keypad input request and response data, the portable reader device 101 will process the request. For either type of data block, the portable reader device 101 sends the command response or the process status back to the PC upon execution of the data block. Once the PC sends out a data block to the interface system, it waits for a response. When a response is received by the PC, it will be processed. Then the program will go and fetch a new command and start the cycle again, until termination. The above routine is presented solely for the purpose of explaining the invention, and other routines could be used within the spirit of the invention, as would be recognized by one skilled in the art. All proprietary rights in the routines described herein are expressly reserved.

Fig. 12 is a block diagram of an embodiment of the invention having an RS-232 PC interface unit 1202, including RS-232 transceiver circuitry 1204, power conditioning/control circuitry 1206, and OKI "SmartPort" 1208 which couples to the PC interface port 820 of portable reader device 101. The unit 1202 connects to an external target system, such as a personal computer (PC) 1210, via RS-232 standard communications. The PC interface unit 1202 is intended to enable connectivity between an IC card and a personal computer (PC). The portable reader device 101 provides the interface to the IC card 810, while the interface unit 1202 provides the interface to the PC system 1210 through an RS-232 port. The portable reader device 101 is connected with the interface unit 1202 through, for example, a 4-pin port, e.g., the OKI SmartPort 1208. In such an implementation of the invention, IC card commands and data are communicated through 1208 using, for example, the customized communication protocol of the invention. The illustrated PC interface unit includes the RS-232 transceiver circuitry 1204 in order to convert signals from the SmartPort 1208 to RS-232 compatible signals, and includes the power conditioning/control circuitry 1206 in order to provide power to the portable reader device 101 from the PC 1210 while it is operated in the connected mode. With the PC interface unit 1202 installed, the portable reader device 101 detects the existence of the external interface unit 1202 and switches its operation mode to the connected mode, as already mentioned. At that point, the PC 1210 will take full control of the communication with the portable reader device 101.

To initiate communication with the IC card 810, the PC 1210 will, for example, transmit a command to the portable reader device 101 to request a Reset of the IC card 810. The portable reader device 101 will interpret the command it receives from the SmartPort 1208, and initiate the Reset of the IC card 810. If the Reset of the IC card 810 is successful, and the portable reader device 101 receives ATR (Answer to Reset) bytes from the IC card 810, it will in turn send an ATR response back to the PC.

As mentioned before, there are two variations of

operational method for the system in the connected mode: a pass-through method and a non-pass-through method. These communication methods and sequences are applicable for all the different interface systems described herein. The only difference among the several interface systems is the choice of communication medium and path.

Fig. 13 is a block diagram of an embodiment of the invention having an infra-red (IrDA) interface unit 1302 which couples to an external target system 1304 via infrared signals. The unit 1302 includes a SmartPort 1306 which couples to the IC card portable reader device 101, power control circuitry 1308, UART/MCU 1310, LCD display 1312, modulation circuit 1314, transmitter (LED) 1316, receiver (photo-diode) 1318, demodulator 1320, and input module 1322. The IrDA interface system 1302 provides signal conversion from digital data coming out of the portable reader device 101 to IrDA compatible signals.

Fig. 14 is a block diagram of an embodiment of the invention having a radio frequency (RF) interface unit 1402, including a UART/MCU 1408 which interfaces to the portable reader device 101 through SmartPort 1410, power control circuitry 1402, digital signal processor (DSP) 1414, an analog RF block 1416 with power amplifier frequency synthesis receiver and filter, and transceiver 1418. Communication with the external target system 1404 in this case is through radio communication between antennas 1406, e.g., a cellular network. An LCD display 1420 and an input module 1422 are also provided. The RF interface system converts digital signals from the portable reader device 101 to an analog signal from the digital data signal, and then to an RF (modulated) signal for use in transmission through the air by way of an antenna 1406. A coaxial RF transmission could of course also be implemented if desired. Further, any of a variety of known RF techniques could be used within the spirit of the invention.

When the IR (infra-red light) interface module 1302 or the RF (radio frequency) interface module 1402 is used, the modular system enables the IC card data to be transferred through an IR or an RF medium, respectively, to the external target device 1404.

Fig. 15 is a block diagram of an embodiment of the invention having a modem interface unit 1502, which includes SmartPort 1504 coupling the unit to the portable reader device 101, power control circuitry 1506, an LCD display 1508, an input module 1510, UART/MCU 1512, a modem chip set 1514, and a transceiver circuit 1516. The unit couples to a target system through a public system telephone network 1518. The modem interface system 1502 provides signal conversion from digital data signals from the IC card 810 through the portable reader device 101 to signals compatible with the public system telephone network (PSTN) 1518.

Fig. 16 is a diagram of an embodiment of the invention having a modular interface unit 1602 such as one of the types previously described, the diagram being for showing the three layers of communication protocol: Application, Transport and Physical layers. This overview of the ValueChecker+ modular interface system shows a generic interface system 1602 designed according to the invention. The block diagram also illustrates various connectivity methods for the several embodiments of the system, and the tri-level communications protocol is specified. A block diagram of the portable reader device 101 is also shown in this figure as well.

The invention takes advantage of a modular interface design as should have been apparent from the preceding description. A special command protocol, mentioned above, is used with the interface system. The command protocol is used to provide a standardized command syntax for communication between the external system 1604 and the MCU 806 in the portable reader device 101.

Below is a detailed description of an exemplary command protocol according to an embodiment of the invention.

As was previously mentioned, the command protocol used in the device PC interface is similar to the Type 1 block transfer protocol in the ISO 7816 part 3. Each data block according to the invention has a header, a length byte to indicate the total length of the subsequent data bytes, and a duplication of the header byte, optional data bytes and the final checksum byte that is equal to the XOR of all the proceeding bytes within the block. All the values for the command block are coded in Hex digits.

There are two modes of IC card (ICC) Command and Response data interchange between the portable reader device and the host PC. The first mode is the pass-through mode. In this mode, the host PC takes care of all the block framing, block sequence number tracking and error handling. The data sent out from the host PC to the portable reader device 101 is the exact command data the portable reader device 101 will send to the IC card 810. Also, the response resulting from the execution of the command will be sent back to the host PC without any modification. This mode is intended for the situation where the host PC takes direct control over the IC card 810.

The second mode is the non-pass-through mode. In this mode, the portable reader device 101 handles the command framing, sequence number tracking and error handling. The data sent out from the host PC is only the raw APDU command bytes, and the portable reader device 101 returns only the final response, e.g., data plus status word, from the command execution to the host PC.

Simplifying change calculations for IC card cash purchases is another object of the disclosed invention. The solution will now be described in more detail with reference to Figs. 17 to 20.

A personal IC card portable reader device 101 containing a micro-controller 806 and support circuitry,

power supply (batteries 210), display 104, IC/smart card communications hardware (port 808) and software, and a simple keypad 106K, has been described above. The portable reader device 101 is constructed so that the user's IC card 810 is inserted and stored in a slot 108 in the portable reader device 101, and so that the user can easily and quickly perform interactions with the data stored on the card 810. In the Background and Summary sections above, the problem of determining how much available value (electronic cash balance) should be left in the IC card 810 after a purchase, has been discussed, and a solution summarized.

Prior to making a purchase, the user would turn on the portable reader device 101, whereupon it would immediately display the remaining balance on the card (standalone/passive mode). At that point, the user can push a function button, the "Check-Change" button, to start a procedure to calculate the expected remaining balance after his anticipated purchase.

After pushing the "Check-Change" button, the user enters the amount of the planned purchase using the numbered keys followed by the "enter" key. At this point the portable reader device will calculate and display the expected balance on the card following the purchase.

Upon completing the purchase and receiving the card back from the retailer, the user returns the card to his reader device and turns the portable reader device on, thereby displaying the remaining balance on the card. The user can then easily visually verify that the correct purchase amount has been deducted from the card and the remaining balance is correct. Fig. 17 shows a flow chart for this first operational sequence, a first embodiment of a change-checking method according to the invention. Fig. 18 is a flow chart for a first alternate embodiment of a change-checking method according to the invention, Fig. 19 is a flow chart for a second alternate embodiment of a change-checking method according to the invention, and Fig. 20 is a flow chart for a third alternate embodiment of a change-checking method according to the invention. The method in Fig. 20 is similar to the method in Fig. 17, except that in addition, the device stores the expected purchase and original balance amounts, and a validation is provided for by pressing the "Check-Change" function button to validate the final balance after the purchase, by subtracting the purchase amount from the original balance.

The proposed solution according to an exemplary embodiment of the invention offers several distinct advantages over using a calculator to determine the expected remaining balance after a purchase. The entry for the starting and ending balances of the card is automatic upon insertion into the reader (standalone/passive mode), and does not have to be manually entered into a calculator by the user. This not only saves time, but considerably reduces the chance of error. Further, the card reading function and change calculation functions are combined into one compact, easy to use unit, eliminating the need for separate card reader and calculator device.

Other alternative embodiments which are considered to be within the scope of the invention are now mentioned. The solution may also be accomplished with simple variations of the above described preferred embodiment. These include:

1) Calculating the correct starting balance based on the final balance and purchase amount. The user enters the purchase price based on the final remaining balance, and verifies that the calculated starting balance matches the original balance shown (see Fig. 18).

2) The IC card reader device stores the starting balance and ending balance, and calculates the expected purchase value. The user then verifies that the expected purchase amount corresponds to the actual purchase amount (see Fig. 19).

3) Alternatively, the portable reader device can be made such that the comparisons are made automatically rather than through activation by the user. For instance, the portable reader device stores the initial balance in memory, the user enters the expected purchase amount, and the user makes the purchase. When the card is returned to the portable reader device after the purchase, the portable reader device reads and records the final card balance, and indicates to the user that this ending balance is correct (Fig. 20).

This invention proposes a simple solution to the problem of verifying the correct purchase amount and expected balance when using IC card/smart card electronic cash for purchases. It combines a card reader with a keypad in such a way that the user can quickly and accurately verify the expected balance on his or her card following a purchase.

Fig. 21 is a schematic diagram for an embodiment of an interface unit according to the invention and Fig. 22 is a schematic of an embodiment of the IC card portable reader device 101 according to the invention.

The portable reader device 101 in the illustrated exemplary preferred embodiment is contemplated to support only T=0 and T=1 IC cards. However, support for other types of memory cards could be added within the spirit of the invention.

The modular IC card interface system can be summarized as including two basic components, the portable reader device 101 and the interface module 600 (see e.g., Figs. 6, 8 and 12). The portable reader device 101 includes all the necessary electrical circuitry to interface with an IC card 810, an output module, e.g., a liquid crystal display (LCD) 104 for data output display, an input module, e.g., a keypad 104, and an interface port 820. The interface port 820 is the same for the portable reader device 101, and all the interface modules to which it may be connected to, e.g., an RS-232 module

802/1202, a modem module 1502, an RF module 1402, an IR module 1302, or any other specialized modules which could be useful, such as a printer interface module, for example. By connecting different interface modules to the portable reader device 101, the IC card data can be transferred through different communication channels as required. A specialized command protocol is used to provide a common protocol for all the interface modules regardless of the medium, which will be described in detail later.

As mentioned above, according to an exemplary embodiment of the invention, there are three modes of operation, a standalone/passive mode which provides a static data display, a standalone/active mode which allows expanded functions, and a connected mode in which an external system, e.g., a personal computer (PC), takes control of the device.

In the connected mode, power may be supplied from external source via the interface module, e.g., from a PC via the RS-232 interface unit 1202. Further, in the connected mode, the LCD 104 and keypad 106K in the portable reader device 101, can be controlled by an external application program. The interface module takes care of signal conversion, and the portable reader device 101 does not need adjustment to accommodate different interface modules, i.e., a change of interface modules is transparent to the portable reader device 101 for data transfers.

Uses for the interface include, but are not limited to, the following :

Home Banking with a PC - the user can employ the interface system along with a modem-equipped PC to download funds from his/her bank account to the IC card, or to update the transaction profile stored in the IC card.

Access Control - the user can use an IC card to gain access to a computer network or another place. This is accomplished by using the interface system to provide a link for authentication data residing in an IC card to be validated by an external terminal.

Data logging - data can be communicated between an IC card and a terminal through the interface system, enabling various other applications to be implemented.

It will be apparent to one skilled in the art that the manner of making written description of the preferred embodiments, taken together with the drawings.

It will be understood that the above description of the preferred embodiment of the present invention is susceptible to various modifications, changes, and adaptations, and the same are intended to be comprehended within the meaning and range of equivalents of the invention.

Although the disclosed embodiments relate to providing a serial interface, the invention is not limited to such, but may also provide a parallel interface as required for a particular application.

Claims

1. A portable IC card reader device, comprising:

   a compact housing, including a portion which accommodates at least one battery;
   a keypad, disposed in the housing, having numeric keys and function keys;
   a display, disposed in the housing, which displays alpha-numeric characters; and
   electronic circuitry, disposed in the housing, interconnecting the keypad and display;
   wherein the electronic circuitry includes a micro-controller, an IC card port, and an input/output port; and
   wherein the micro-controller is operative to control reading and writing to and from an IC card, and to perform functions related to IC card transactions.

2. The reader device according to claim 1, further comprising an interface module which couples to the input/output port and interfaces the reader device with an external device over a communications medium.

3. The reader device according to claim 2, wherein the interface module is a serial interface module, the module comprising a housing, serial transceiver circuitry disposed in the housing, a first input/output connector which connects to the input/output port of the reader device, a cable coupling the connector to the transceiver circuitry, and a second input/output connector which couples the serial interface module transceiver to an external device.

4. The reader device according to claim 3, wherein the serial interface module transceiver circuitry comprises RS-232 transceiver circuitry.

5. The reader device according to claim 3, wherein the serial interface module transceiver circuitry comprises infra-red transceiver circuitry.

6. The reader device according to claim 3, wherein the serial interface module transceiver circuitry comprises radio-frequency transceiver circuitry.

7. The reader device according to claim 3, wherein the serial interface module transceiver circuitry comprises modem circuitry.

8. A method of operating a portable IC card reading device according to claim 1, comprising:

   reading a stored value from an IC card when the IC card is inserted in the device;
   receiving user input corresponding to an

amount of a planned purchase;
automatically calculating and displaying an expected balance after the planned purchase; and
after making the planned purchase with the IC card, reading a stored value from an IC card when the IC card is inserted in the device, and displaying the value read.

9. A method of operating a portable IC card reading device according to claim 1, comprising:

reading a first stored value from an IC card when the IC card is inserted in the device prior to being used to make a purchase by a user;
reading a second stored value from the IC card when the IC card is inserted in the device after being used to make the purchase by the user; and
automatically calculating and displaying a purchase price based on the first and second stored values.

10. A method of operating a portable IC card reading device according to claim 1, comprising:

reading a first stored value from an IC card when the IC card is inserted in the device prior to being used to make a purchase by a user;
receiving user input corresponding to an amount of a purchase;
reading a second stored value from an IC card when the IC card is inserted in the device after being used to make the purchase by the user; and
automatically verifying the first stored value corresponds to the second stored value minus the purchase amount.

11. A portable IC card reader device, comprising:

a compact housing having a form factor sized to fit in a shirt pocket or wallet;
keyed input means for receiving keyed-in user input data;
display means for displaying data to a user;
IC card reading/writing means for reading/writing to/from an IC card;
processing and control means for processing data and controlling operations of the reader device; and
interface means for interfacing the IC card reader device with an external device for the exchange of at least data.

12. The reader device according to claim 11, wherein the display means comprises a liquid crystal display device.

13. The reader device according to claim 11, wherein the keyed input means comprises a pin-pad keypad having a plurality of keys including numeric and function keys.

14. The reader device according to claim 11, wherein the processing means comprises a micro-controller.

15. The reader device according to claim 11, wherein the interface means comprises an input/output port.

16. The reader device according to claim 15, further comprising an interface module which couples to the input/output port and interfaces the reader device with an external device over a communications medium.

17. The portable IC card reader device according to claim 1, wherein the portion which accommodates at least one battery comprises a removable battery tray.

18. The portable IC card reader device according to claim 17, wherein the removable battery tray comprises first and second battery compartments for receiving a respective battery therein, and battery contacts for connecting batteries received in the battery tray to the electronic circuitry of the device.

19. The reader device according to claim 11, wherein the device has a plurality of modes of operation, including:

standalone passive mode, wherein the reader device is not connected to any adapter and simply displays data read from an IC card;
standalone active mode, wherein the reader device is not connected to any adapter, accepts and responds to user commands input on the keyed input means, and interacts with an IC card according to the user commands;
connected pass-through mode, wherein the reader device is connected to an adapter, the adapter is connected to an external host or controller device, and the external host or controller controls the reader device; and
connected non-pass-through mode, wherein the reader device is connected to an adapter, the adapter is connected to an external host or controller device, and the reader device performs some operations independently of the external host or controller device.

20. The reader device according to claim 19, wherein the device has a communications protocol for communicating with external devices, the protocol provides for:

communicating with a plurality of different external adapter devices;

operating in any of said modes of operation;

handling a plurality of reader operations, including IC card interfacing, display of information on said display means, power management, and keypad entry on said keyed entry means; and

communications error handling and status.

21. In a portable IC card reader device, a printed circuit board arrangement comprising:

a housing having first and second parallel planar surfaces; and

a printed circuit board disposed in the housing, including a substrate having a thickness of about 0.020 in. (0.5mm), and including a portion which engages an external connector through an opening in the housing;

wherein the printed circuit board is held by the housing at a first position, parallel to and between the planar surfaces of the housing, at the opening in the housing, and is held at a second position different from the first position, parallel to the planar surfaces of the housing and adjacent to the first parallel planar surface of the housing, the printed circuit board having a flex region between the first position and the second position.

22. The printed circuit board arrangement according to claim 21, wherein at the first position, the printed circuit board extends in a direction substantially perpendicular to an edge of the housing at the opening in the housing.

23. The printed circuit board arrangement according to claim 21, wherein the portion which engages the external connector comprises four electrical contacts.

24. The printed circuit board arrangement according to claim 23, wherein the external connector is a four pin molex connector and wherein the portion which engages the external connector is adapted to mate with a four pin molex connector.

25. An interface module for a portable IC card reader device, comprising:

a housing;

serial transceiver circuitry disposed in the housing;

a first input/output connector which connects to an input/output port of the portable IC card reader;

a cable coupling the connector to the transceiver circuitry; and

a second input/output port which couples the serial interface module transceiver to an external device.

26. The interface module according to claim 25, wherein the serial interface module transceiver circuitry comprises RS-232 transceiver circuitry.

27. The interface module according to claim 25, wherein the serial interface module transceiver circuitry comprises infra-red transceiver circuitry.

28. The interface module according to claim 25, wherein the serial interface module transceiver circuitry comprises radio-frequency transceiver circuitry.

29. The interface module according to claim 25, wherein the serial interface module transceiver circuitry comprises modem circuitry.

30. A method of operating a portable IC card reading device ,comprising:

reading a stored value from an IC card when the IC card is inserted in the device;

receiving user input corresponding to an amount of a planned purchase; and

calculating and displaying an expected balance after the planned purchase.

31. The method according to claim 30, further comprising:

after making a purchase with the IC card, reading a stored value from the IC card when the IC card is inserted in the device, and displaying the value read.

32. A method of operating a portable IC card reading device, comprising:

reading a first stored value from an IC card when the IC card is inserted in the device prior to being used by a user to make a purchase;

reading a second stored value from the IC card when the IC card is inserted in the device after being used by a user to make the purchase; and

calculating and displaying a purchase price based on the first and second stored values.

33. A method of operating a portable IC card reading device, comprising:

reading a first stored value from an IC card when the IC card is inserted in the device prior

to being used by a user to make a purchase;

receiving user input corresponding to an amount of a purchase;

reading a second stored value from the IC card when the IC card is inserted in the device after being used by a user to make the purchase; and

verifying the first stored value corresponds to the second stored value minus the purchase amount.

34. A portable modular IC card interface system, comprising:

a compact portable personal IC card reader; and

a plurality of different interface modules.

35. The system of claim 34, wherein the reader comprises:

a housing;

IC card interface circuitry and hardware;

a user keypad;

a user information display;

an interface port for connecting the reader to the plurality of different interface modules; and

an internal power source.

36. The system of claim 34, wherein the plurality of different interface modules include:

an RS232 interface module;

an infra-red interface module;

a telephone network interface module; and

a radio-frequency interface module.

37. The system of claim 34, wherein the system uses a communications protocol that facilitates communications with the plurality of different interface modules through the interface port.

38. The system of claim 34, wherein the system has a plurality of operating modes, the modes including:

standalone passive mode;

standalone active mode; and

connected mode;

wherein, when the reader is not connected to an external device through any of the plurality of different interface modules, the reader operates in the standalone passive mode or the standalone active mode;

wherein, in the standalone passive mode, the reader operates to display data from an IC card to a user;

wherein in the standalone active mode, the reader operates to receive user input and interact with an IC card based on the user input; and

wherein in the connected mode, the reader device operates either interactively or passively with an external device to interface the external device to an IC card.

39. The system of claim 38, wherein, when in the connected mode, the external device can control the reader keypad and display, and can control an IC card inserted in the reader.

40. The system of claim 39, wherein the system uses a common communications protocol that facilitates communications with the external device through any one of the plurality of different interface modules through the interface port.

41. The system of claim 40, wherein the protocol comprises a data block having at least three fields, the fields comprising"

a header and length information field;

an optional information/data field; and

a checksum field.

42. The system of claim 41, wherein the header and length information field comprises a function/command, wherein length data indicates the presence of and size of data associated with the command/function.

43. The system of claim 42, wherein the function/command comprises at least one of a display control command; a keypad entry control, status, and reference inquiry; and IC card communication.

44. The system of claim 34, wherein the plurality of different interface modules provide for communication at a plurality of baud rates.

45. The system of claim 34, wherein power can be provided to the reader through any one of the plurality of different interface modules.

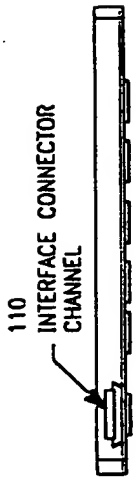


FIG. 1A

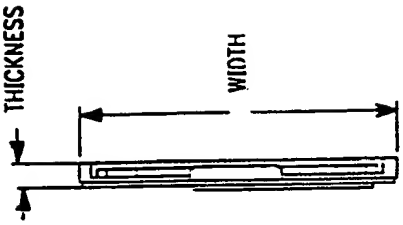


FIG. 1B

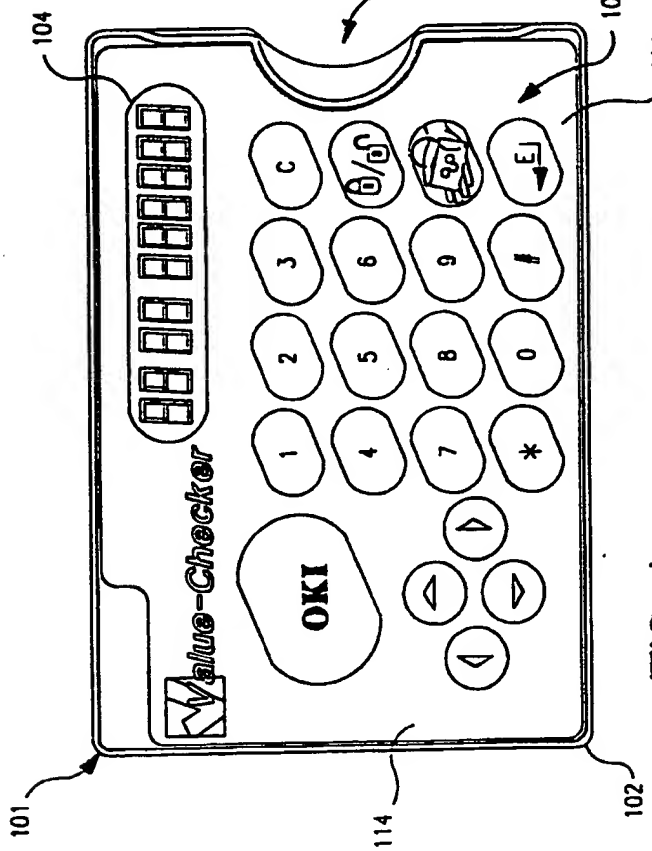


FIG. 1

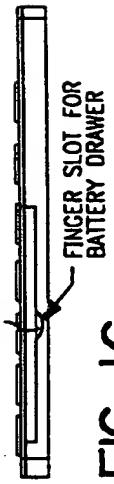


FIG. 1C

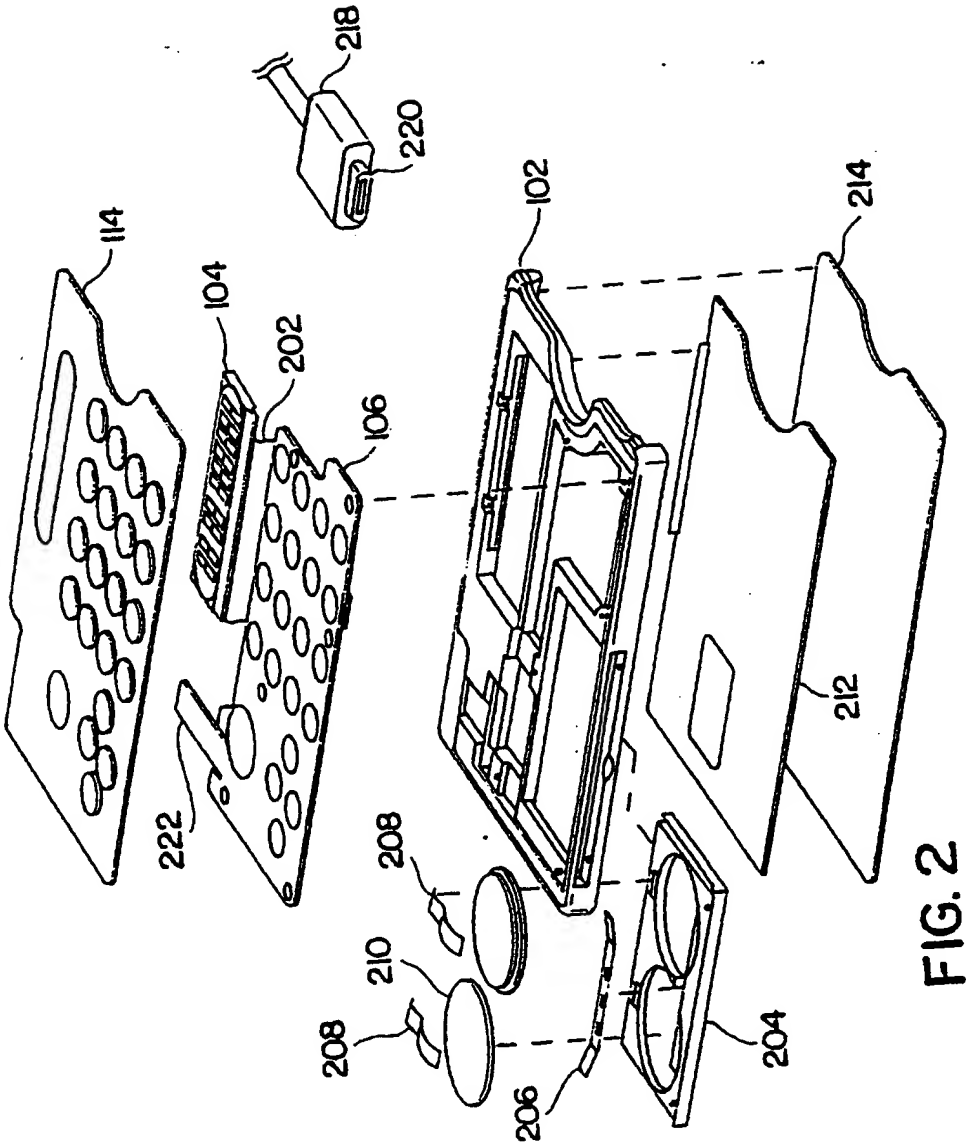


FIG. 2

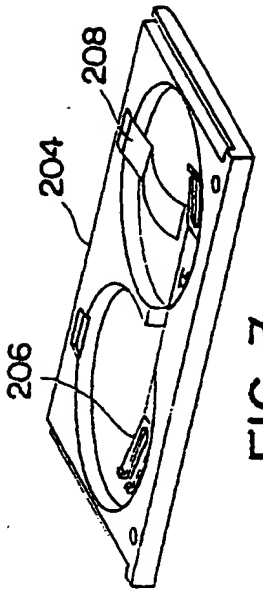


FIG. 3

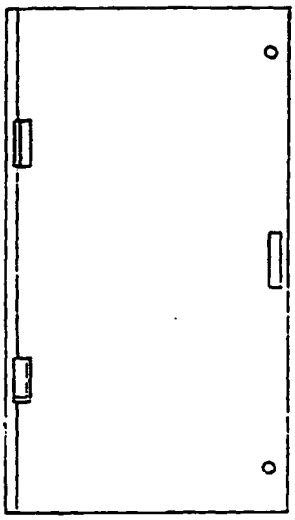


FIG. 3F

FIG. 3E

FIG. 3A

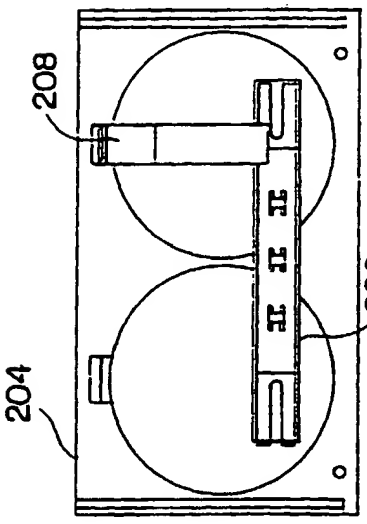


FIG. 3C

FIG. 3D

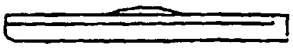


FIG. 3B

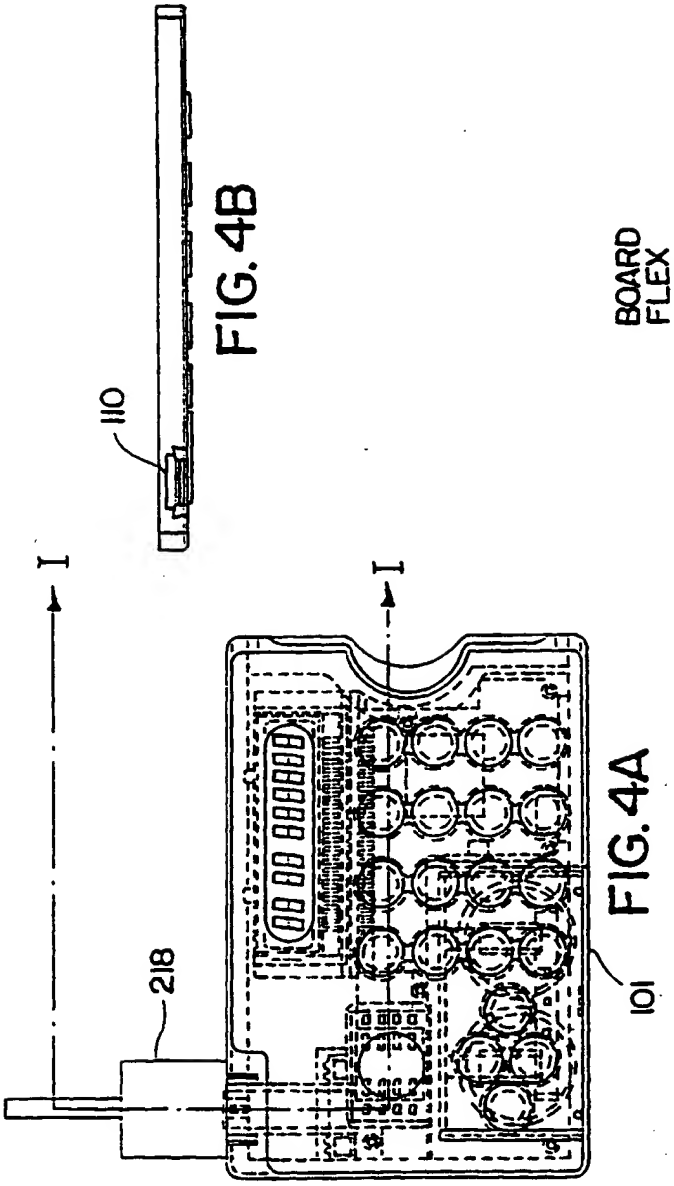


FIG. 4B

FIG. 4A

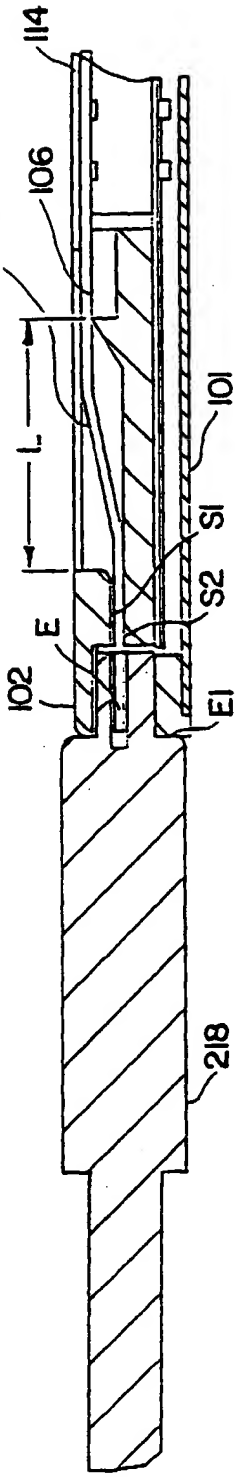


FIG. 5

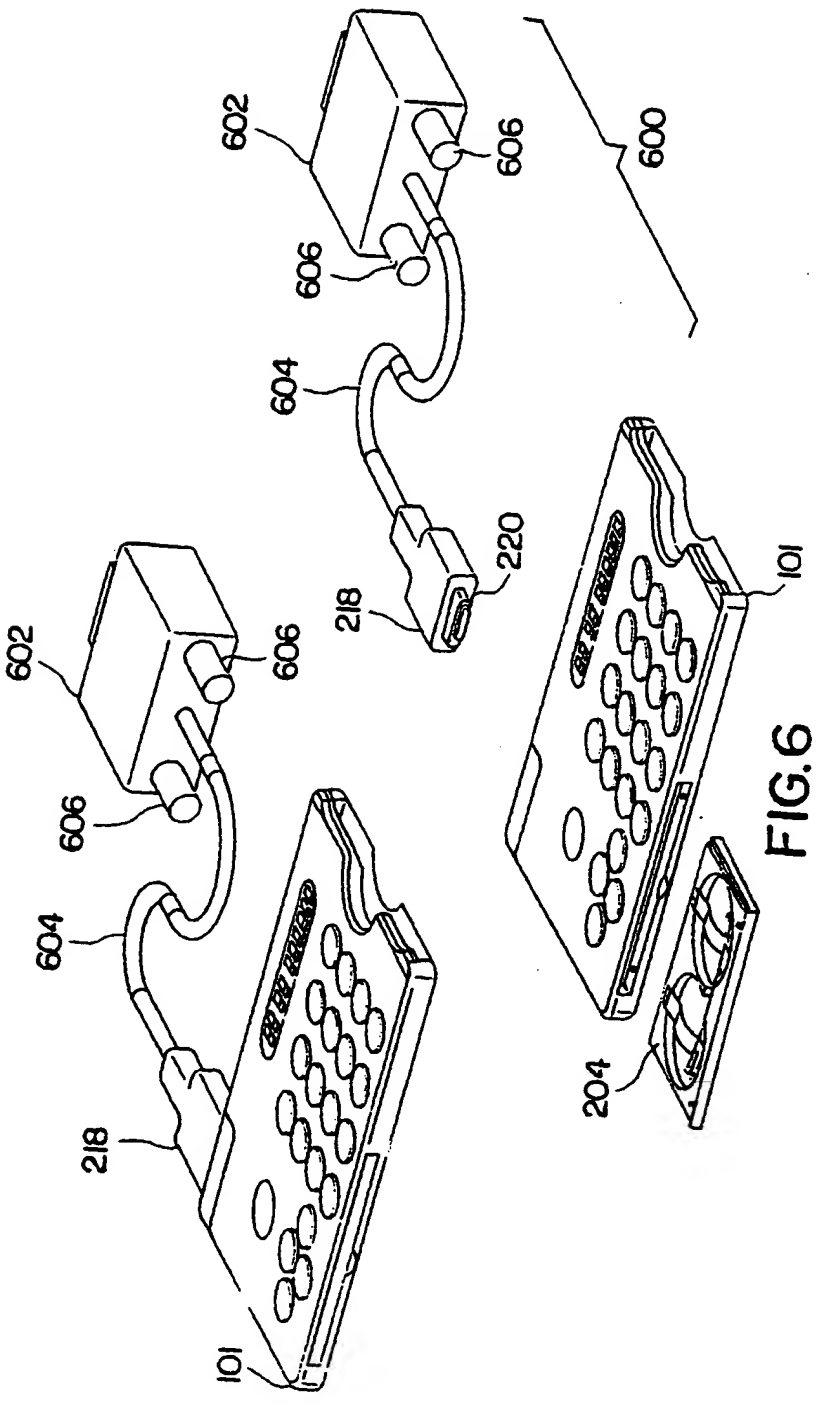


FIG.6

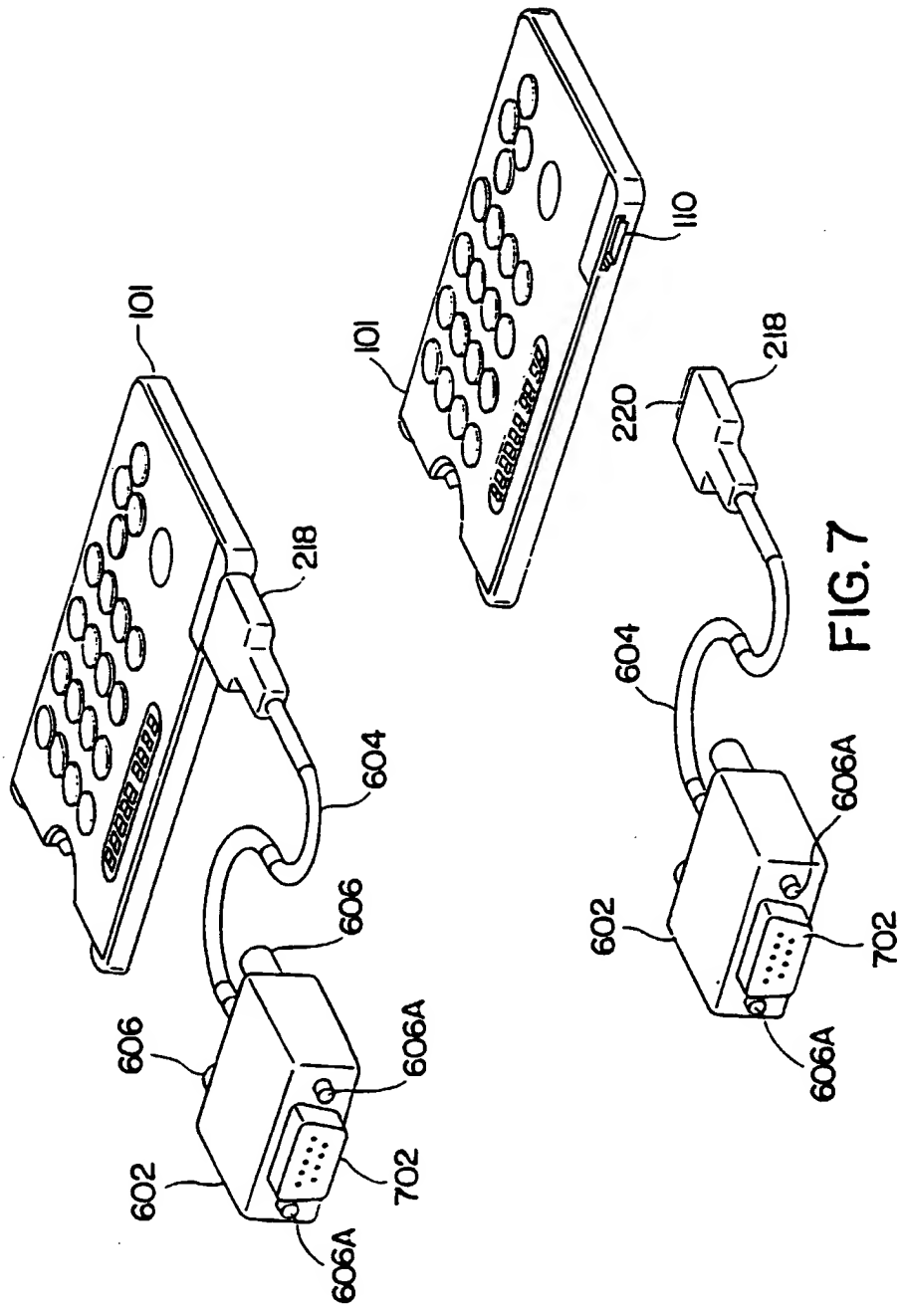

101
218
604
606
606A
602
702
606A
101
110
218
220
604
606A
602
702
606A

FIG. 7

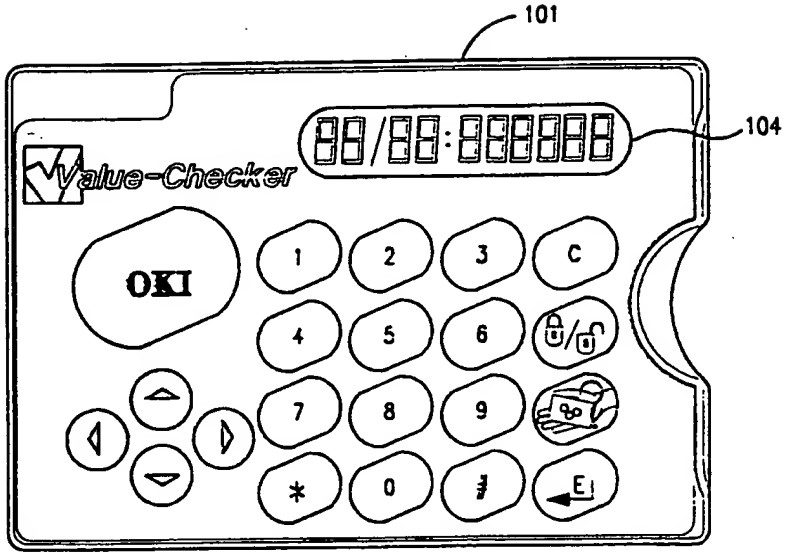

101
104
Value-Checker
OKI
1
2
3
C
4
5
6
7
8
9
*
0
#
E

FIG. 8A

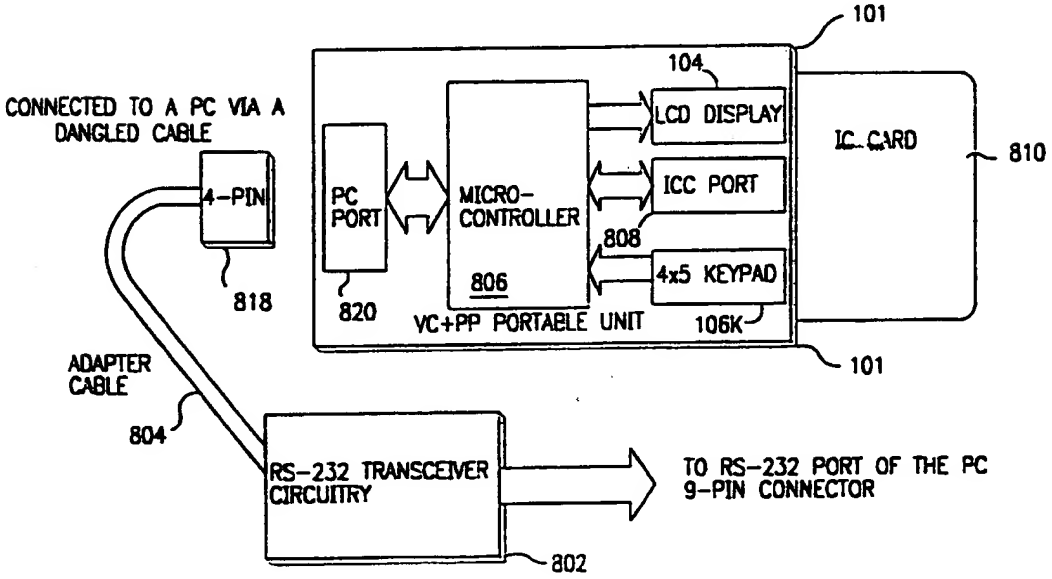

101
104
CONNECTED TO A PC VIA A DANGLED CABLE
4-PIN
818
PC PORT
820
MICRO-CONTROLLER
806
LCD DISPLAY
ICC PORT
808
4x5 KEYPAD
106K
VC+PP PORTABLE UNIT
IC CARD
810
101
ADAPTER CABLE
804
RS-232 TRANSCEIVER CIRCUITRY
802
TO RS-232 PORT OF THE PC 9-PIN CONNECTOR

FIG. 8B

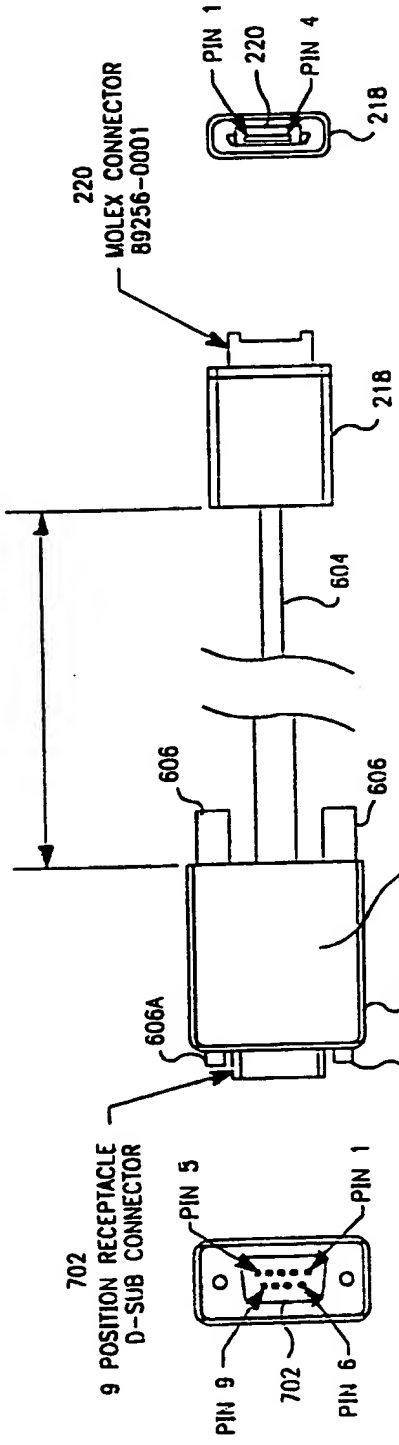


FIG. 9C

FIG. 9A

FIG. 9B

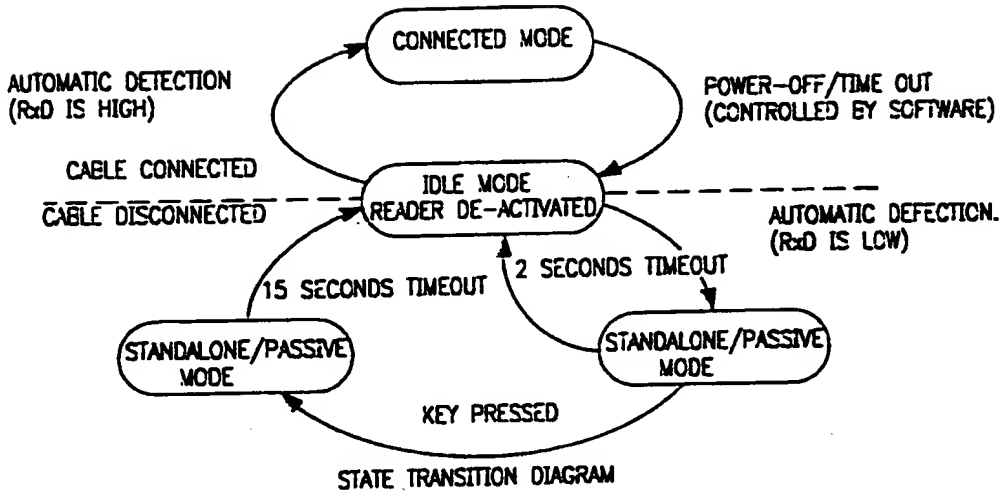

CONNECTED MODE
AUTOMATIC DETECTION
(RxD IS HIGH)
POWER-OFF/TIME OUT
(CONTROLLED BY SOFTWARE)
CABLE CONNECTED
CABLE DISCONNECTED
IDLE MODE
READER DE-ACTIVATED
AUTOMATIC DEFECTION.
(RxD IS LOW)
15 SECONDS TIMEOUT
2 SECONDS TIMEOUT
STANDALONE/PASSIVE MODE
STANDALONE/PASSIVE MODE
KEY PRESSED
STATE TRANSITION DIAGRAM

FIG. 10

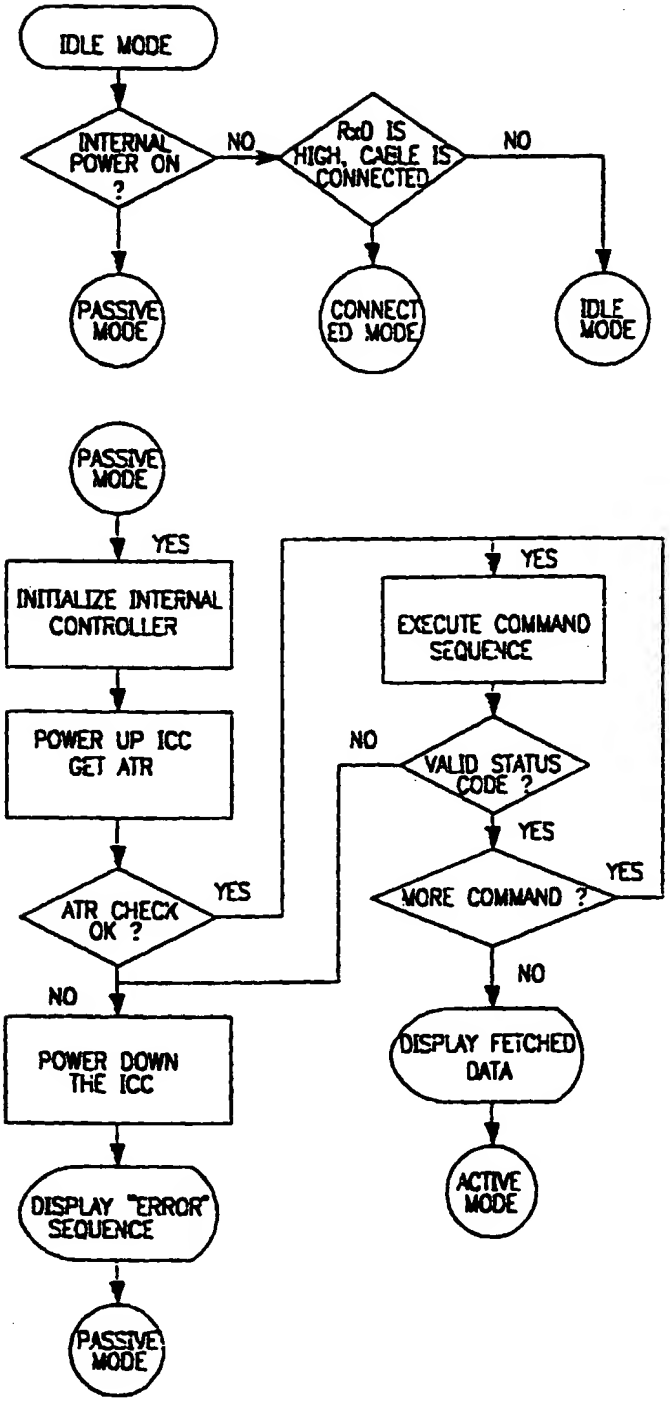

IDLE MODE
INTERNAL POWER ON ?
NO
RxD IS HIGH, CABLE IS CONNECTED
NO
PASSIVE MODE
CONNECTED MODE
IDLE MODE
PASSIVE MODE
YES
INITIALIZE INTERNAL CONTROLLER
POWER UP ICC GET ATR
ATR CHECK OK ?
YES
NO
POWER DOWN THE ICC
DISPLAY "ERROR" SEQUENCE
PASSIVE MODE
YES
EXECUTE COMMAND SEQUENCE
NO
VALID STATUS CODE ?
YES
MORE COMMAND ?
YES
NO
DISPLAY FETCHED DATA
ACTIVE MODE

FIG 10A

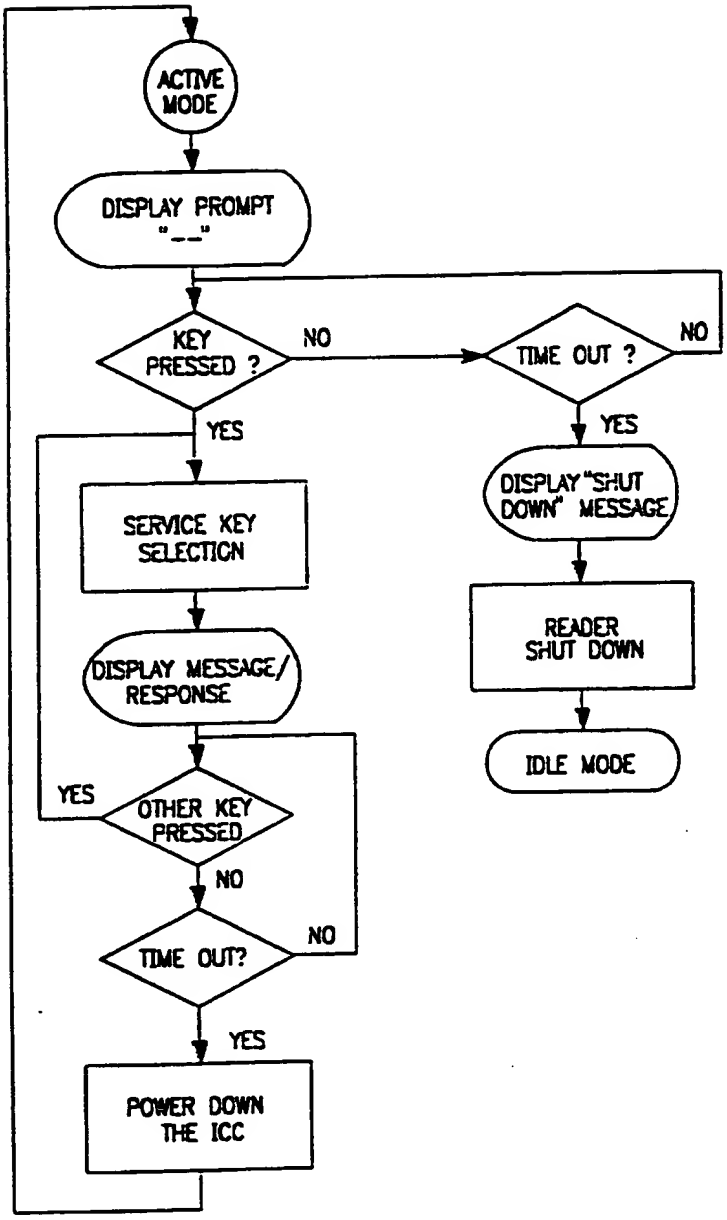

ACTIVE MODE
DISPLAY PROMPT "__"
KEY PRESSED ?
NO
TIME OUT ?
NO
YES
YES
SERVICE KEY SELECTION
DISPLAY "SHUT DOWN" MESSAGE
READER SHUT DOWN
DISPLAY MESSAGE/ RESPONSE
IDLE MODE
YES
OTHER KEY PRESSED
NO
TIME OUT?
NO
YES
POWER DOWN THE ICC

FIG 10B

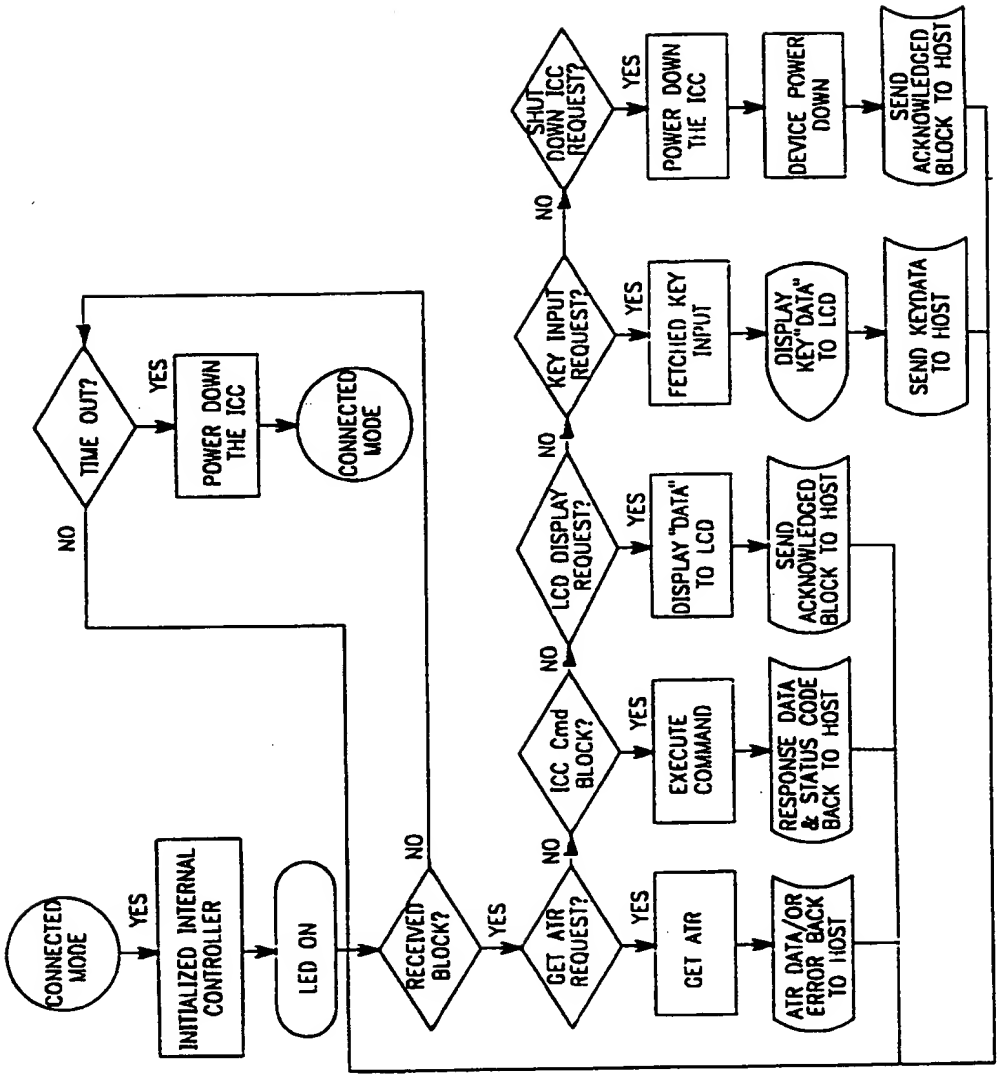

CONNECTED MODE
YES
INITIALIZED INTERNAL CONTROLLER
LED ON
RECEIVED BLOCK?
NO
YES
GET ATR REQUEST?
NO
YES
GET ATR
ATR DATA/OR ERROR BACK TO HOST
ICC Cmd BLOCK?
NO
YES
EXECUTE COMMAND
RESPONSE DATA & STATUS CODE BACK TO HOST
LCD DISPLAY REQUEST?
NO
YES
DISPLAY "DATA" TO LCD
SEND ACKNOWLEDGED BLOCK TO HOST
KEY INPUT REQUEST?
NO
YES
FETCHED KEY INPUT
DISPLAY KEY"DATA" TO LCD
SEND KEYDATA TO HOST
SHUT DOWN ICC REQUEST?
NO
YES
POWER DOWN THE ICC
DEVICE POWER DOWN
SEND ACKNOWLEDGED BLOCK TO HOST
TIME OUT?
NO
YES
POWER DOWN THE ICC
CONNECTED MODE

FIG. 10C

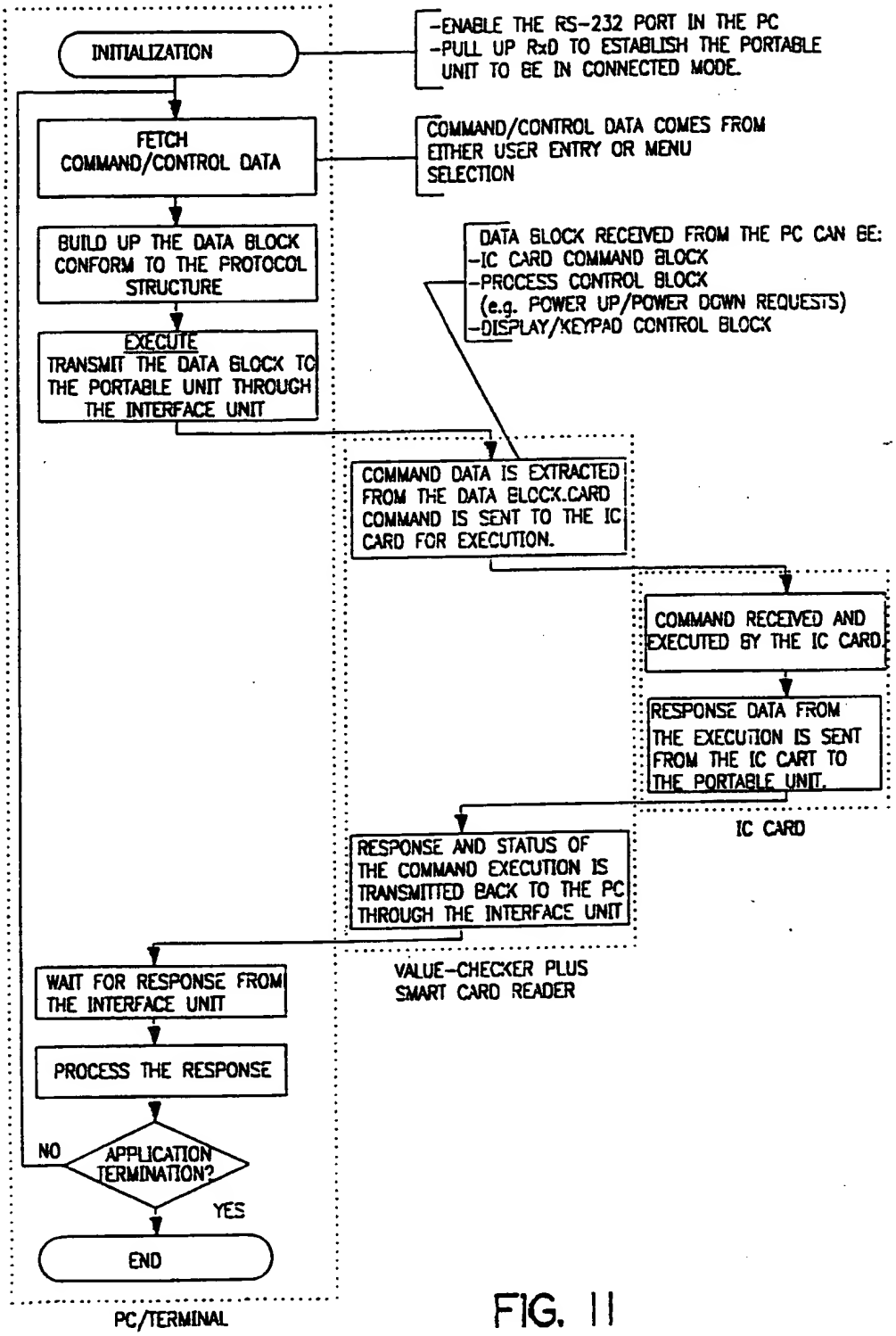

INITIALIZATION
-ENABLE THE RS-232 PORT IN THE PC
-PULL UP RxD TO ESTABLISH THE PORTABLE UNIT TO BE IN CONNECTED MODE.
FETCH COMMAND/CONTROL DATA
COMMAND/CONTROL DATA COMES FROM EITHER USER ENTRY OR MENU SELECTION
BUILD UP THE DATA BLOCK CONFORM TO THE PROTOCOL STRUCTURE
DATA BLOCK RECEIVED FROM THE PC CAN BE:
-IC CARD COMMAND BLOCK
-PROCESS CONTROL BLOCK
(e.g. POWER UP/POWER DOWN REQUESTS)
-DISPLAY/KEYPAD CONTROL BLOCK
EXECUTE
TRANSMIT THE DATA BLOCK TO THE PORTABLE UNIT THROUGH THE INTERFACE UNIT
COMMAND DATA IS EXTRACTED FROM THE DATA BLOCK.CARD COMMAND IS SENT TO THE IC CARD FOR EXECUTION.
COMMAND RECEIVED AND EXECUTED BY THE IC CARD.
RESPONSE DATA FROM THE EXECUTION IS SENT FROM THE IC CART TO THE PORTABLE UNIT.
IC CARD
RESPONSE AND STATUS OF THE COMMAND EXECUTION IS TRANSMITTED BACK TO THE PC THROUGH THE INTERFACE UNIT
VALUE-CHECKER PLUS SMART CARD READER
WAIT FOR RESPONSE FROM THE INTERFACE UNIT
PROCESS THE RESPONSE
NO
APPLICATION TERMINATION?
YES
END
PC/TERMINAL

FIG. 11

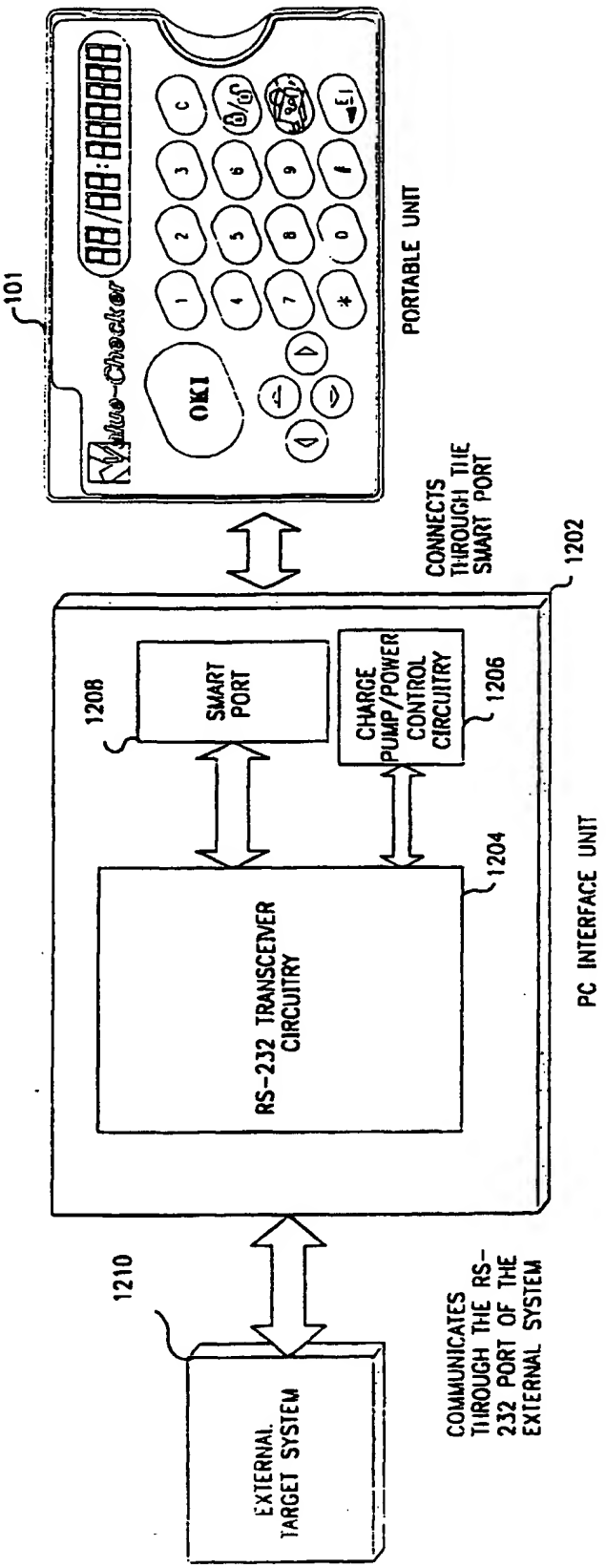

101
Auto-Checker
88/88:888888
OKI
PORTABLE UNIT
CONNECTS THROUGH THE SMART PORT
1202
1208
SMART PORT
CHARGE PUMP/POWER CONTROL CIRCUITRY
1206
1204
RS-232 TRANSCEIVER CIRCUITRY
PC INTERFACE UNIT
1210
EXTERNAL TARGET SYSTEM
COMMUNICATES THROUGH THE RS-232 PORT OF THE EXTERNAL SYSTEM

FIG. 12

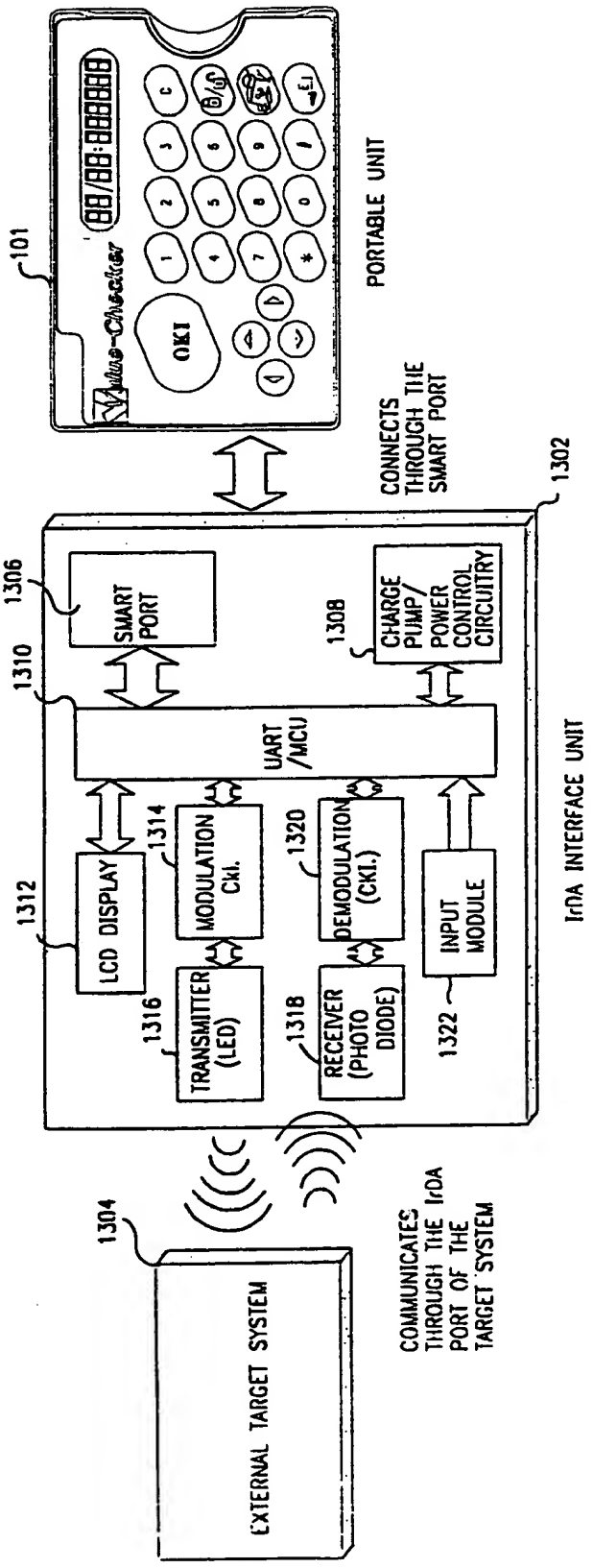

101
PORTABLE UNIT
CONNECTS THROUGH THE SMART PORT
1302
1306
SMART PORT
1308
CHARGE PUMP/ POWER CONTROL CIRCUITRY
1310
UART /MCU
1312
LCD DISPLAY
1314
MODULATION Ckt.
1320
DEMODULATION (Ckt.)
1316
TRANSMITTER (LED)
1318
RECEIVER (PHOTO DIODE)
1322
INPUT MODULE
IrDA INTERFACE UNIT
1304
EXTERNAL TARGET SYSTEM
COMMUNICATES THROUGH THE IrDA PORT OF THE TARGET SYSTEM

FIG. 13

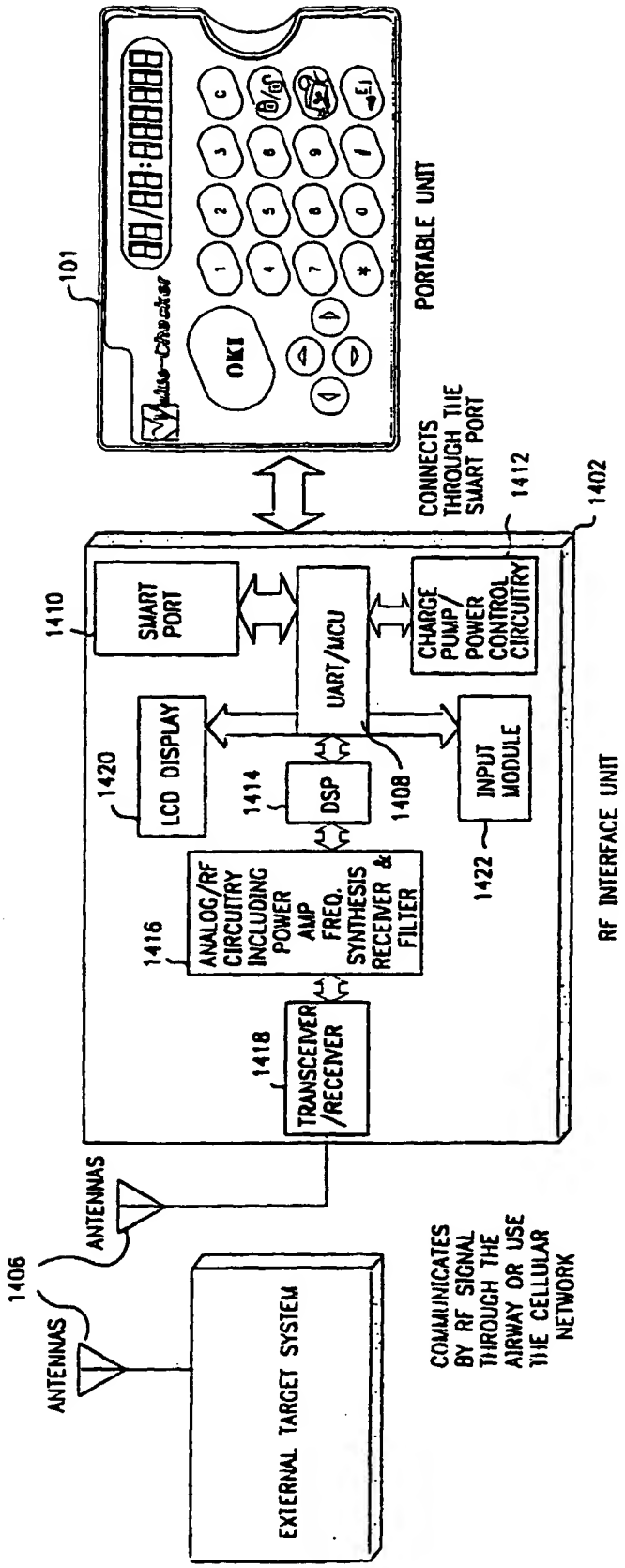

101
PORTABLE UNIT
CONNECTS THROUGH THE SMART PORT
1412
1402
1410
SMART PORT
UART/MCU
CHARGE PUMP/ POWER CONTROL CIRCUITRY
LCD DISPLAY
1420
1414
DSP
1408
INPUT MODULE
1422
1416
ANALOG/RF CIRCUITRY INCLUDING POWER AMP FREQ. SYNTHESIS RECEIVER & FILTER
1418
TRANSCEIVER /RECEIVER
RF INTERFACE UNIT
ANTENNAS
1406
ANTENNAS
EXTERNAL TARGET SYSTEM
COMMUNICATES BY RF SIGNAL THROUGH THE AIRWAY OR USE THE CELLULAR NETWORK

FIG. 14

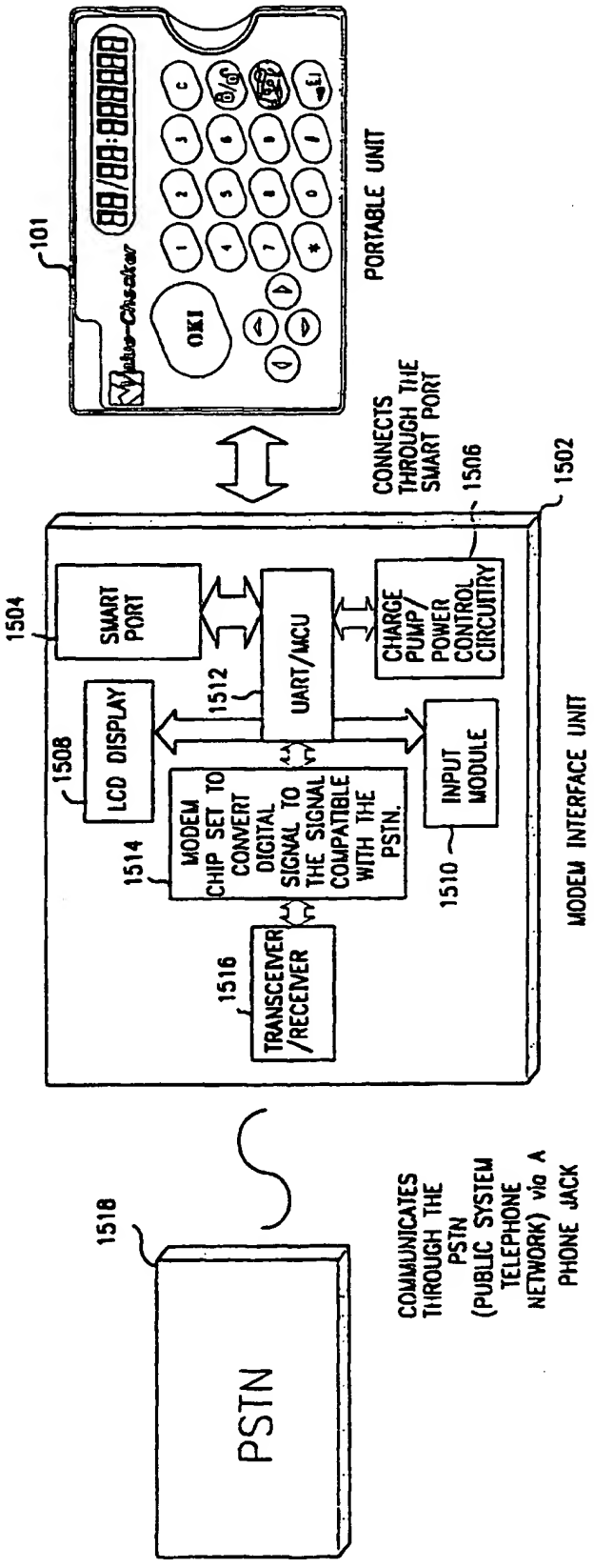

101
PORTABLE UNIT
CONNECTS THROUGH THE SMART PORT
1506
1502
1504
SMART PORT
UART/MCU
CHARGE PUMP/ POWER CONTROL CIRCUITRY
1512
1508
LCD DISPLAY
1514
MODEM CHIP SET TO CONVERT DIGITAL SIGNAL TO THE SIGNAL COMPATIBLE WITH THE PSTN.
1510
INPUT MODULE
1516
TRANSCEIVER /RECEIVER
MODEM INTERFACE UNIT
1518
PSTN
COMMUNICATES THROUGH THE PSTN (PUBLIC SYSTEM TELEPHONE NETWORK) via A PHONE JACK

FIG. 15

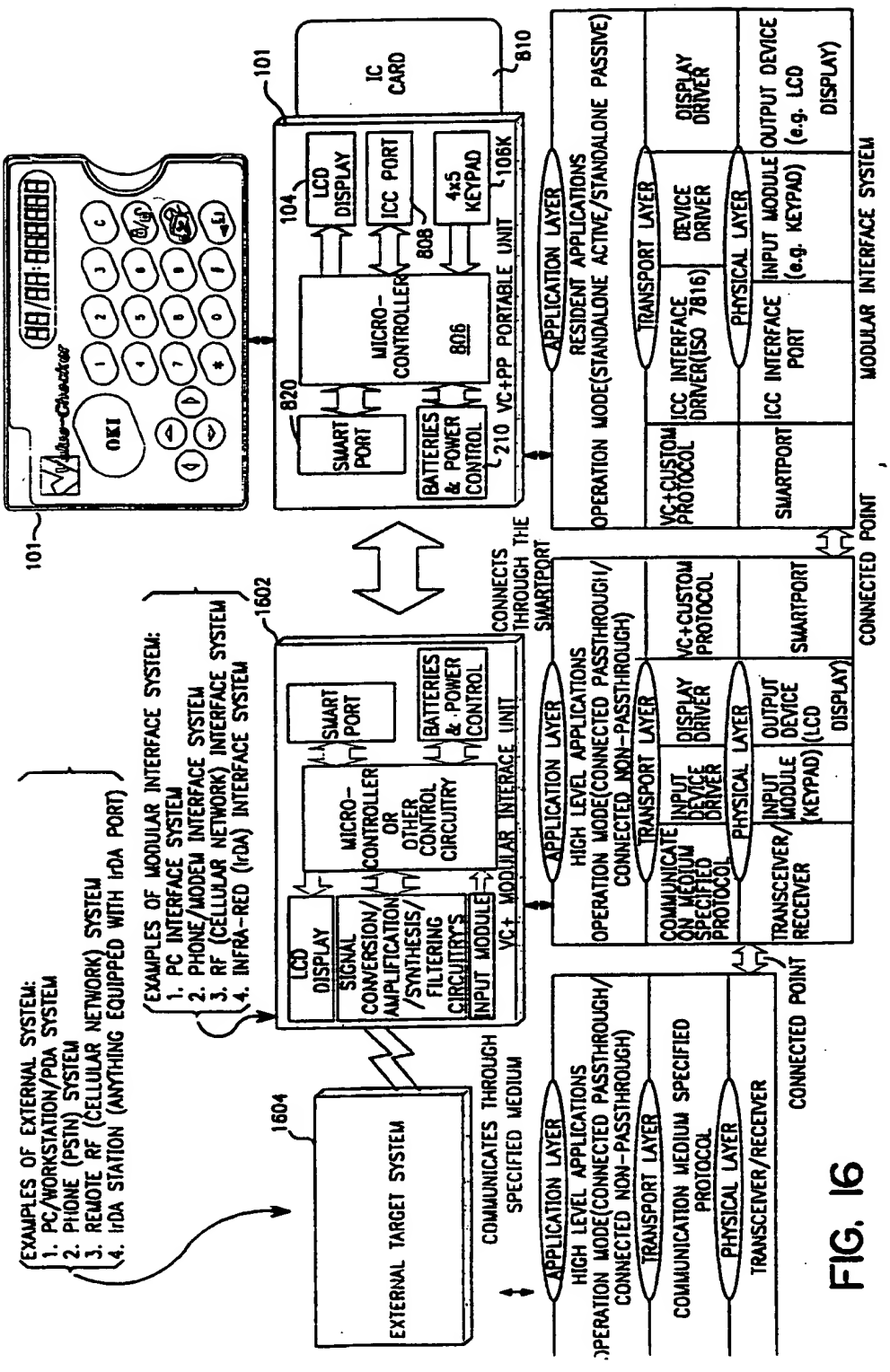

EXAMPLES OF EXTERNAL SYSTEM:
1. PC/WORKSTATION/PDA SYSTEM
2. PHONE (PSTN) SYSTEM
3. REMOTE RF (CELLULAR NETWORK) SYSTEM
4. IrDA STATION (ANYTHING EQUIPPED WITH IrDA PORT)
EXAMPLES OF MODULAR INTERFACE SYSTEM:
1. PC INTERFACE SYSTEM
2. PHONE/MODEM INTERFACE SYSTEM
3. RF (CELLULAR NETWORK) INTERFACE SYSTEM
4. INFRA-RED (IrDA) INTERFACE SYSTEM
101
1602
1604
EXTERNAL TARGET SYSTEM
COMMUNICATES THROUGH SPECIFIED MEDIUM
CONNECTS THROUGH THE SMARTPORT
CONNECTED POINT
MODULAR INTERFACE SYSTEM
LCD DISPLAY
SIGNAL CONVERSION/ AMPLIFICATION /SYNTHESIS/ FILTERING CIRCUITRY'S
MICRO-CONTROLLER OR OTHER CONTROL CIRCUITRY
SMART PORT
BATTERIES & POWER CONTROL
INPUT MODULE
VC+ MODULAR INTERFACE UNIT
APPLICATION LAYER
HIGH LEVEL APPLICATIONS
OPERATION MODE(CONNECTED PASSTHROUGH/ CONNECTED NON-PASSTHROUGH)
TRANSPORT LAYER
COMMUNICATE ON MEDIUM SPECIFIED PROTOCOL
INPUT DEVICE DRIVER
DISPLAY DRIVER
VC+CUSTOM PROTOCOL
PHYSICAL LAYER
TRANSCEIVER/ RECEIVER
INPUT MODULE (KEYPAD)
OUTPUT DEVICE (LCD DISPLAY)
SMARTPORT
OPERATION MODE(STANDALONE ACTIVE/STANDALONE PASSIVE)
RESIDENT APPLICATIONS
VC+CUSTOM PROTOCOL
ICC INTERFACE DRIVER(ISO 7816)
DEVICE DRIVER
ICC INTERFACE PORT
INPUT MODULE (e.g. KEYPAD)
OUTPUT DEVICE (e.g. LCD DISPLAY)
DISPLAY DRIVER
104
LCD DISPLAY
ICC PORT
808
4x5 KEYPAD
106K
MICRO-CONTROLLER
806
820
SMART PORT
BATTERIES & POWER CONTROL
210 VC+PP PORTABLE UNIT
IC CARD
810

FIG. 16

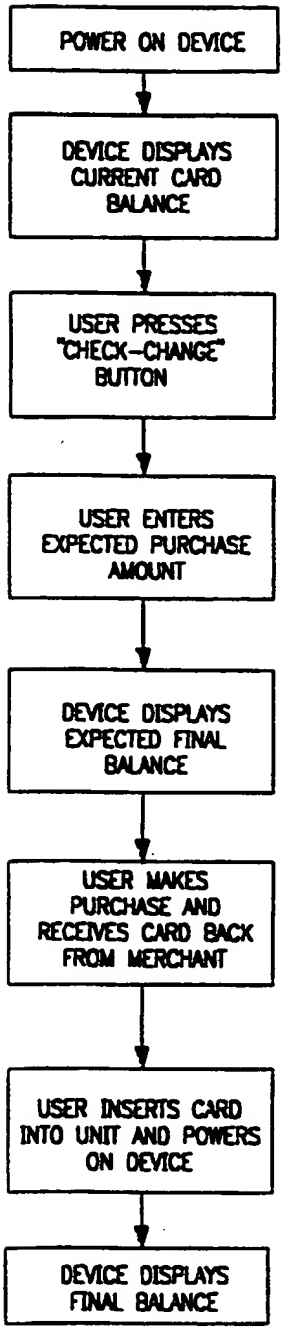


FIG. 17

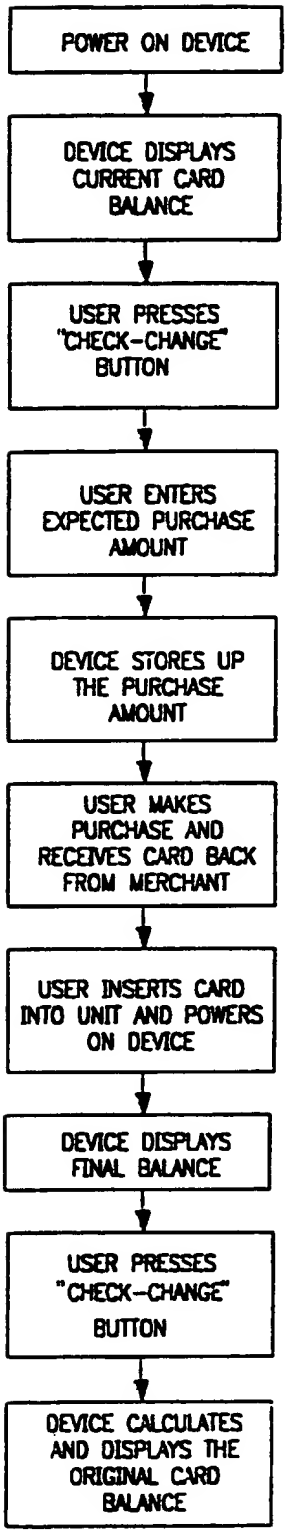


FIG. 18

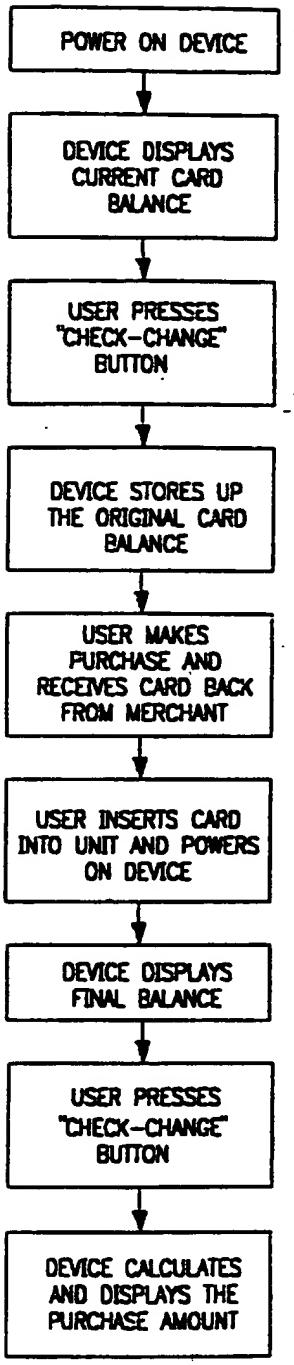


FIG. 19

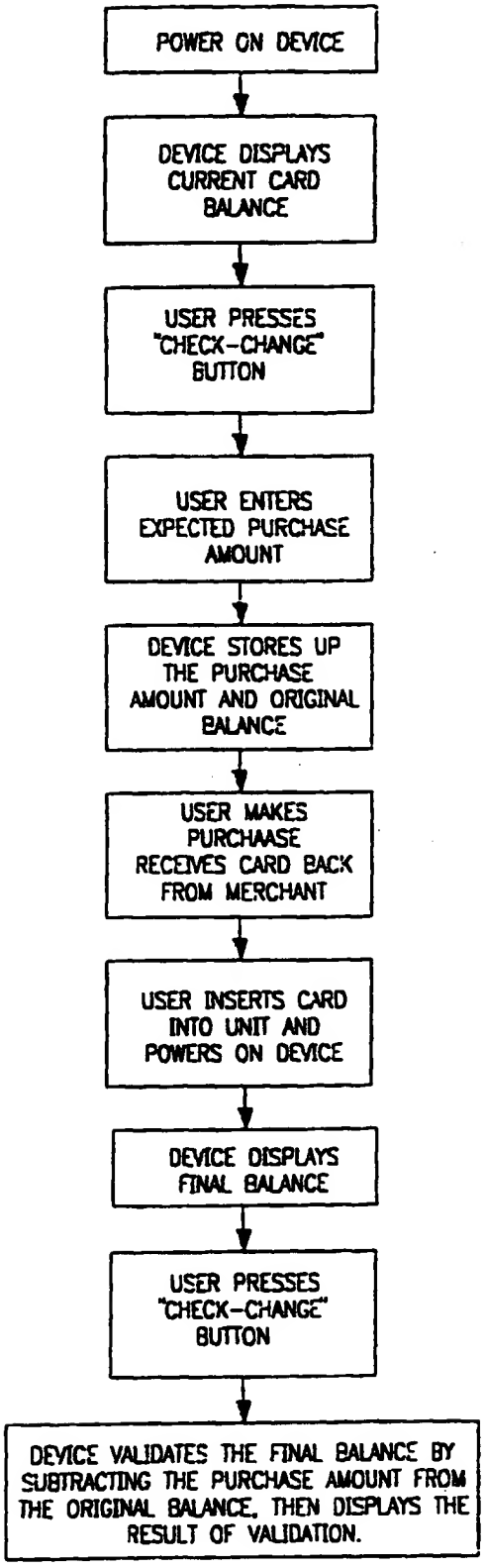

POWER ON DEVICE
DEVICE DISPLAYS CURRENT CARD BALANCE
USER PRESSES "CHECK-CHANGE" BUTTON
USER ENTERS EXPECTED PURCHASE AMOUNT
DEVICE STORES UP THE PURCHASE AMOUNT AND ORIGINAL BALANCE
USER MAKES PURCHAASE RECEIVES CARD BACK FROM MERCHANT
USER INSERTS CARD INTO UNIT AND POWERS ON DEVICE
DEVICE DISPLAYS FINAL BALANCE
USER PRESSES "CHECK-CHANGE" BUTTON
DEVICE VALIDATES THE FINAL BALANCE BY SUBTRACTING THE PURCHASE AMOUNT FROM THE ORIGINAL BALANCE. THEN DISPLAYS THE RESULT OF VALIDATION.

FIG. 20

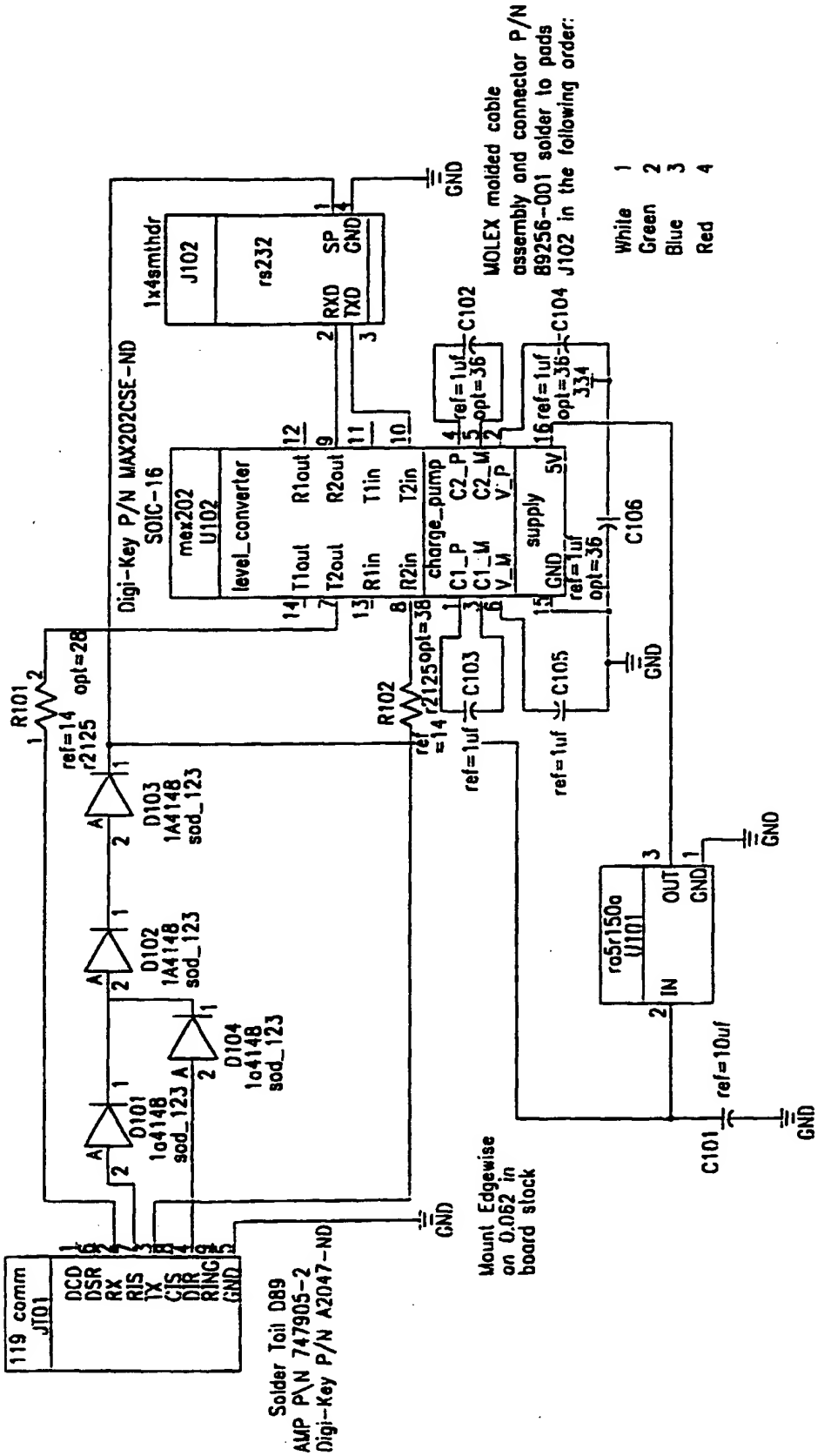

1x4smthdr
J102
rs232
RXD
TXD
SP
GND
GND
MOLEX molded cable assembly and connector P/N 89256-001 solder to pads J102 in the following order:
White 1
Green 2
Blue 3
Red 4
Digi-Key P/N MAX202CSE-ND
SOIC-16
max202
U102
level_converter
T1out
T2out
R1in
R2in
R1out
R2out
T1in
T2in
charge_pump
C1_P
C1_M
V_M
C2_P
C2_M
V_P
supply
5V
GND
C102
ref=1uf
opt=36
C104
ref=1uf
opt=36
334
C106
ref=1uf
opt=36
C103
ref=1uf
C105
ref=1uf
R101
ref=14
r2125
opt=28
R102
ref=14
r2125
opt=38
D103
1A4148
sod_123
D102
1A4148
sod_123
D104
1a4148
sod_123
D101
1a4148
sod_123
119 comm
J101
DCD
DSR
RX
RTS
TX
CTS
DIR
RING
GND
Solder Tail D89
AMP P\N 747905-2
Digi-Key P/N A2047-ND
Mount Edgewise
on 0.062 in
board stock
ra5r150a
U101
IN
OUT
GND
C101
ref=10uf

FIG. 21

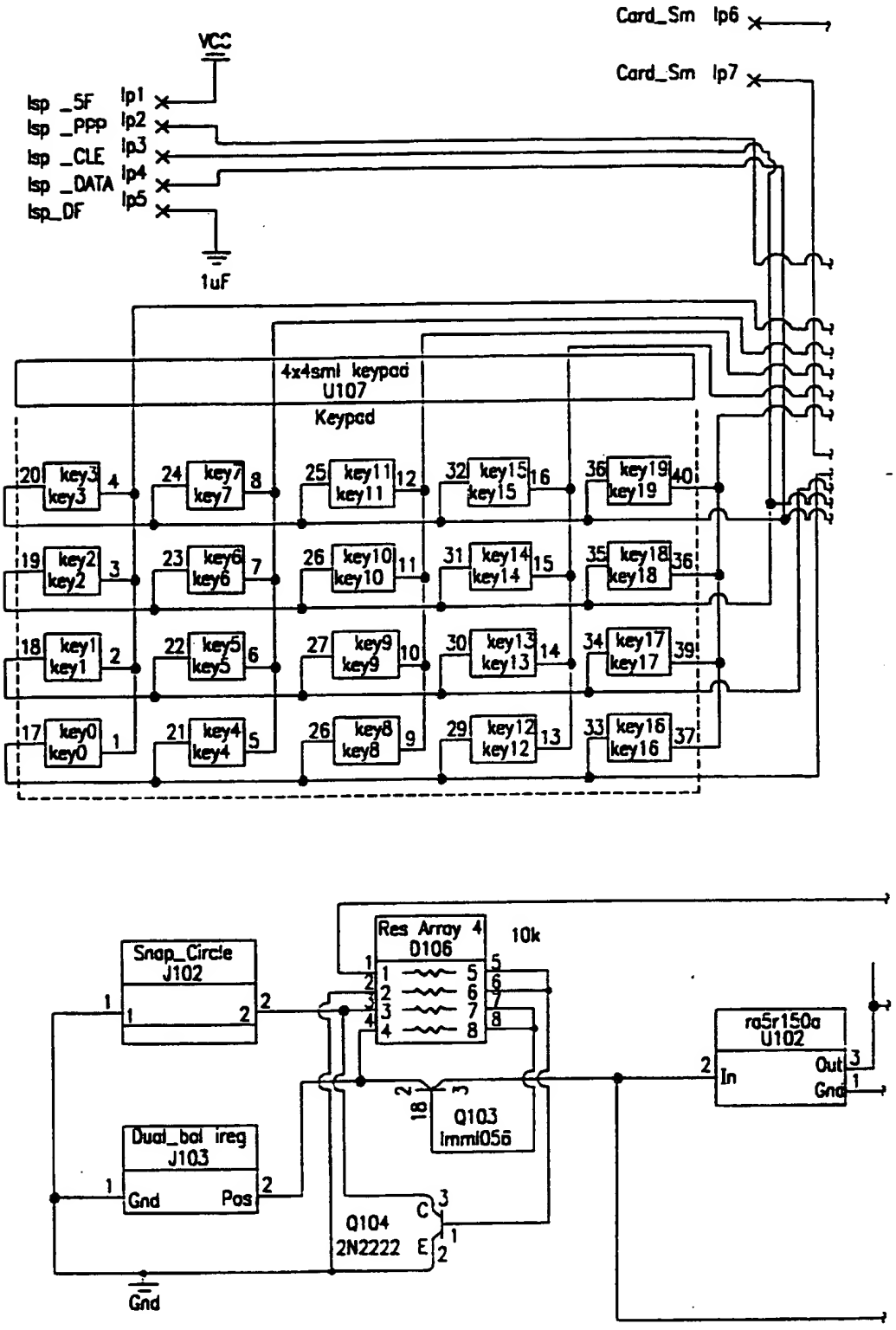

VCC
lsp _SF
lsp _PPP
lsp _CLE
lsp _DATA
lsp_DF
Ip1
Ip2
Ip3
Ip4
Ip5
1uF
Card_Sm Ip6
Card_Sm Ip7
4x4sml keypad
U107
Keypad
key3
key7
key11
key15
key19
key2
key6
key10
key14
key18
key1
key5
key9
key13
key17
key0
key4
key8
key12
key16
Snap_Circle
J102
Res Array 4
D106
10k
Dual_bat ireg
J103
Gnd
Pos
Q103
Imml056
Q104
2N2222
ra5r150a
U102
In
Out
Gnd

FIG. 22A

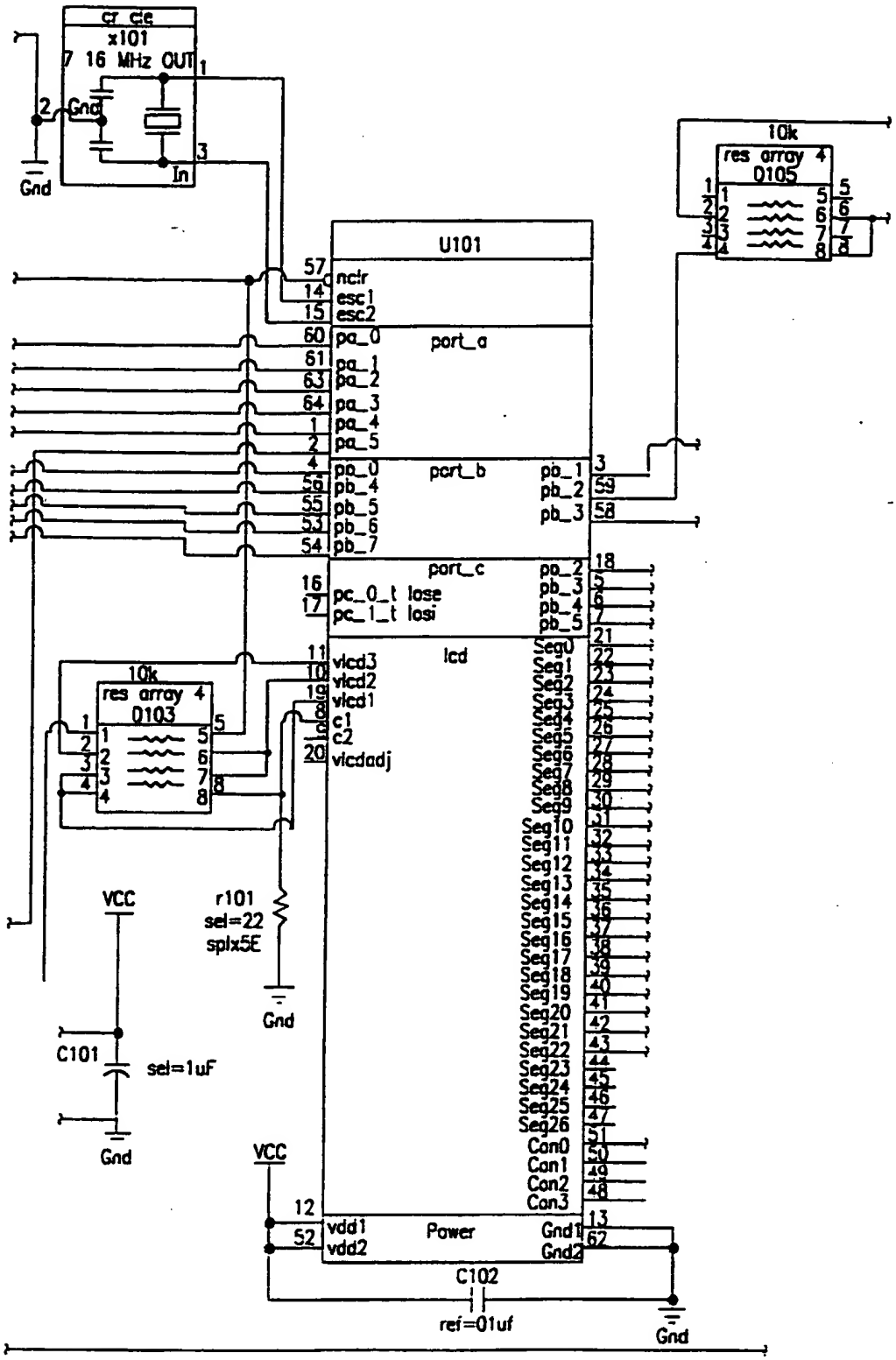

cr_cie
x101
7 16 MHz OUT
Gnd
In
10k
res array 4
0105
U101
nclr
esc1
esc2
port_a
pa_0
pa_1
pa_2
pa_3
pa_4
pa_5
port_b
pb_0
pb_1
pb_2
pb_3
pb_4
pb_5
pb_6
pb_7
port_c
pc_0_t lose
pc_1_t losi
pa_2
pb_3
pb_4
pb_5
lcd
vlcd3
vlcd2
vlcd1
c1
c2
vlcdadj
Seg0
Seg1
Seg2
Seg3
Seg4
Seg5
Seg6
Seg7
Seg8
Seg9
Seg10
Seg11
Seg12
Seg13
Seg14
Seg15
Seg16
Seg17
Seg18
Seg19
Seg20
Seg21
Seg22
Seg23
Seg24
Seg25
Seg26
Com0
Com1
Com2
Com3
10k
res array 4
0103
VCC
r101
sel=22
splx5E
C101
sel=1uF
Gnd
VCC
vdd1
vdd2
Power
Gnd1
Gnd2
C102
ref=01uf

FIG. 22B

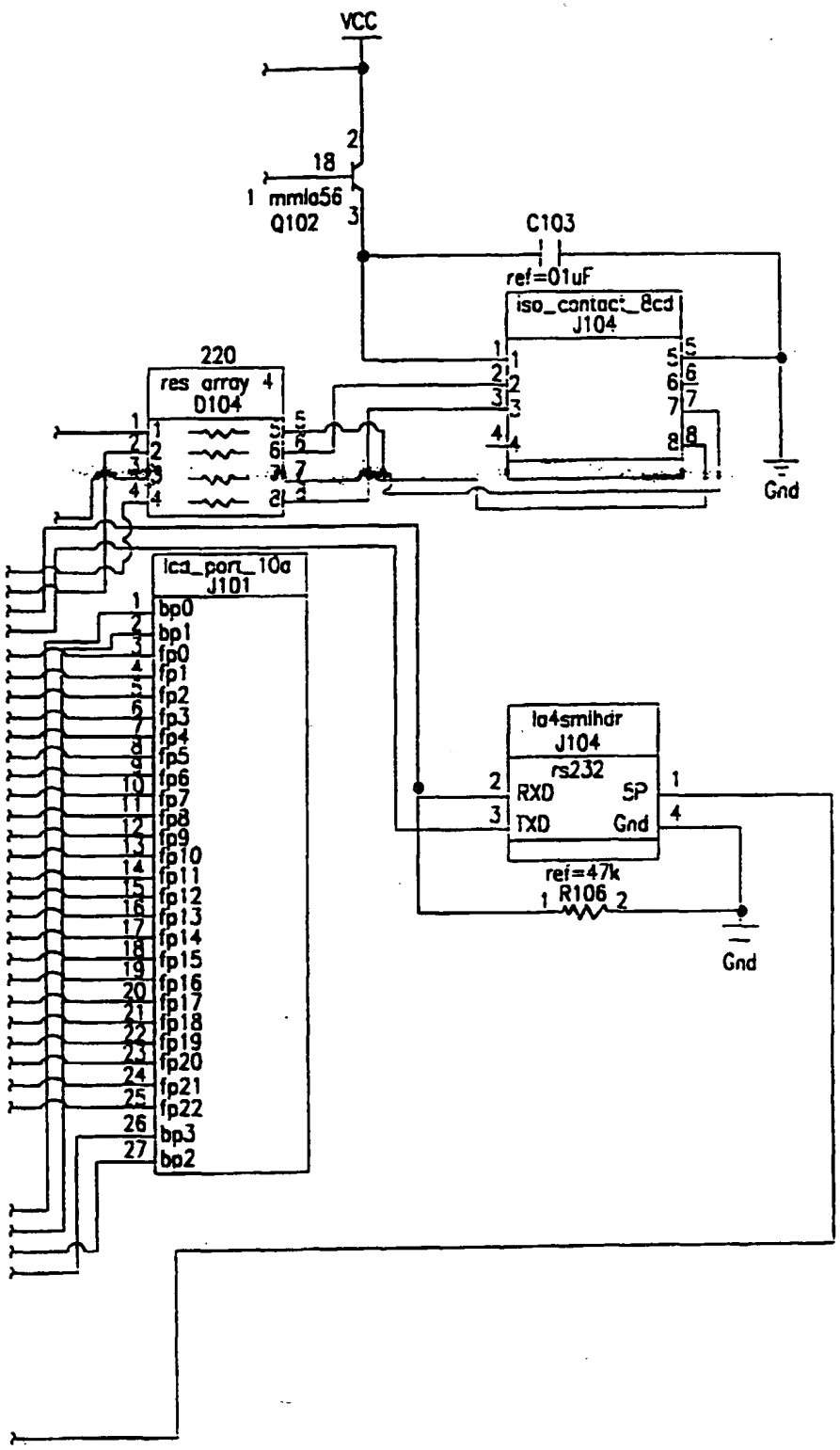

VCC
2
18
1 mmla56
Q102 3
C103
ref=01uF
iso_contact_8cd
J104
220
res array 4
D104
Gnd
lca_port_10a
J101
bp0
bp1
fp0
fp1
fp2
fp3
fp4
fp5
fp6
fp7
fp8
fp9
fp10
fp11
fp12
fp13
fp14
fp15
fp16
fp17
fp18
fp19
fp20
fp21
fp22
bp3
bp2
la4smlhdr
J104
rs232
RXD
TXD
SP
Gnd
ref=47k
R106
Gnd

FIG. 22C

18/5/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007697860 **Image available**
WPI Acc No: 1988-331792/198847
XRPX Acc No: N88-251475
Secure and flexible loading system for smart card **- has execute only program which mutually authenticates loading computer and loads** application program
Patent Assignee: GENERAL ELECTRIC CO PLC (ENGE)
Inventor: EDMONDS R; STEINER A F
Number of Countries: 015 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 292248	A	19881123	EP 88304475	A	19880518	198847	B
GB 2204973	A	19881123	GB 8711744	A	19870519	198847	
AU 8816434	A	19881124				198903	
NO 8802140	A	19881212				198904	
ZA 8803412	A	19890222				198914	

Priority Applications (No Type Date): GB 8711744 A 19870519
Cited Patents: 1.Jnl.Ref; A3...9044; EP 159651; EP 193920; EP 198642; EP 217654; EP 89876; GB 2087606; GB 2168831; JP 61211788; No-SR.Pub; US 3996449; US 4663707; WO 8707060; WO 8707061
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 292248	A	E	6		

Designated States (Regional): AT BE CH DE ES FR GB IT LI LU NL SE

Abstract (Basic): EP 292248 A
The loading system is for the **application program** onto a **smart card** in which the card is coupled to a loading computer which supplies the **program** after **mutual authentication** has taken place. The authenticating and loading **program** is written during manufacture and is execute only.
The **program** can be kept till it is required to change. Alternatively the first loading can be followed by a **program** change, so that the **program** cannot be changed once written Thus flexibility and security can be traded. The system can have an E2 PROM for the read/write regions or it can be a battery-backed ROM.
USE/ADVANTAGE - Esp. **smart card** where flexibility is required. Enables various **application programs** to be written on basic manufactured card and, if necessary, changed.
Title Terms: SECURE; FLEXIBLE; LOAD; SYSTEM; SMART; CARD; EXECUTE; **PROGRAM** ; MUTUAL; LOAD; COMPUTER; LOAD; APPLY; **PROGRAM**
Derwent Class: T01; T04
International Patent Class (Additional): **G06F-003/06** ; **G06F-009/06** ; G07F-007/10; G11C-007/00; G11C-017/00
File Segment: EPI

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 292 248**
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 88304475.2

(22) Date of filing: 18.05.88

(51) Int. Cl.4: G 07 F 7/10
G 07 F 7/08

(30) Priority: 19.05.87 GB 8711744

(43) Date of publication of application:
23.11.88 Bulletin 88/47

(84) Designated Contracting States:
AT BE CH DE ES FR GR IT LI LU NL SE

(71) Applicant: The General Electric Company, p.l.c.
1 Stanhope Gate
London W1A 1EH (GB)

(72) Inventor: Steiner, Anthony Francis
89 Coval Lane
Chelmsford Essex (GB)

Edmonds, Richard
35 Coverside Road
Great Glen Leicester LE8 0EB (GB)

(74) Representative: Tolfree, Roger Keith
GEC p.l.c. Central Patent Department Chelmsford Office
Marconi Research Centre West Hanningfield Road
Great Baddow Chelmsford Essex CM2 8HN (GB)

(54) Data processing system.

(57) The memory area within an electronic token of the 'smart card' type comprising a processor (4), memory (7, 8, 9) and input/output means (5) is divided into an execute only region and a non-volatile read/write region.

A method of loading an applications program is described in which the program is loaded into a portion of the read/write region by software methods and in which the application program may be altered if the use of the card alters.

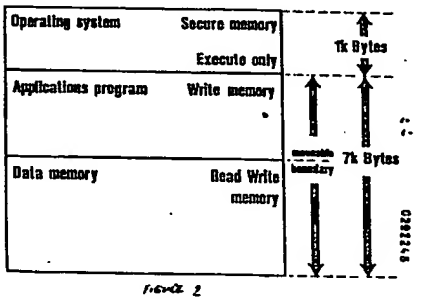


Fig. 2

EP 0 292 248 A2

Description

Data processing System

This invention relates to a data processing system of the type comprising one or more portable electronic tokens, each comprising processing means, memory means and input/output means and one or more fixed read/write terminals, and in particular but not exclusively it relates to such a system as is disclosed in United Kingdom published patent application number GB2173623A, which is incorporated herein by reference.

Transactions between such tokens, often known as 'smart cards' and the read/write terminals are performed under the control of software, known as applications software, residing in both the card and the terminals. The algorithms implemented by the applications software in the card generally determines in full the operation of the card. Conventionally, the application software is embedded into the card at manufacture and is contained within a ROM such that it can not be altered. Each ROM is therefore designed with a particular program and application in mind and to change the ROM, and hence the use of the card, necessitates a considerable expenditure and time and requires new masks to be made.

The present invention arose from the need to produce a card, the software within which is relatively easily changeable to satisfy each different application of the card.

According to the present invention in a first aspect there is provided a method of loading software into a portable electronic token of the type comprising processing means, memory means and input/output means and adapted for interaction with a read/write terminal, wherein the memory means comprises an execute only or read only memory region and a non-volatile read/write region, which method comprises operatively coupling the token and terminal, interchanging messages, under control of an operating system stored in the execute or read only region, between the token and terminal to check whether the token and terminal are authorised, and, only if authorisation is established; loading a program code adapted to form an application program into a portion of the read/write memory region; establishing a partition between the loaded application program and the remainder of the read/write memory region, thus leaving the remainder of the read/write region free for data storage.

In a preferred embodiment, the token is adapted to interact with the terminal by inductive coupling and such coupling is used to load the applications software.

The position of the partition can be varied dependent upon the envisaged uses of the token. The application software will then remain within the electronic token even when it is not operatively coupled to a terminal, until it is wished to load a new program.

Advantageously, the execute only memory region may include within it software such that after applications software has been loaded into the read/write region, checked and tested, the software routine alters, by means of software or hardware, the circuitry within the token such that the applications program is permanently stored within the token and may not be removed or altered by means of the loading procedure described above.

In a second aspect the invention provides an electronic system comprising portable electronic token comprising processing means, memory means and input/output means and a read/write terminal for interacting with the token, wherein the memory means and input/output means a read/write terminal for interacting with the token, wherein the memory means comprises an execute only or Read only memory region and a non-volatile read/write memory region and wherein applications software is stored in a variable size portion of the read/write region.

The Read/write region may be an E^2PROM, battery-barked RAM or any other appropriate non-volatile Read/Write memory.

Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings in which,

Figure 1 shows in block form elements of the electronic token and coupler embodying the present invention and

Figure 2 shows the arrangement of memory areas within the token.

Referring to Figure 1 the general arrangement of an electronic token or card system is shown. A host computer 1 which may be a personal computer (PC) is connected to a coupler unit 2. This unit is arranged to inductively couple with a portable electronic token, shown here as card 3. This is a small hand-held token, perhaps of credit-card sized proportion. Coupling between the card and coupler is achieved inductively by means of modulated fields, as is described in the aforementioned British patent application no. GB2173623A. Card 3 comprises a micro-processor 4 of any convenient type, a Receive/Transmit circuit 5 and power supply means 6 which may either be an on board battery or, more preferably, means for tapping off power which is inductively coupled from the coupler 2. The card further includes a memory region which is divided, according to the invention, into three areas; an operating system area 7, applications program area 8 and data storage area 9. Operating system area 7 is of execute only type and areas 8 and 9 are of non volatile read/write memory, and may for instance be E^2 ROM or battery-backed RAM.

Operating system, application program and data storage may occupy adjacent areas of memory within one integrated circuit. The microprocessor and memory may be embodied in a single integrated circuit.

The coupler 2 comprises a demodulator 10 and modulator 11 for processing modulated signals received or transmitted after amplification by an amplifier 12. Unmodulated signals, either after

demodulation or before modulation are fed to or from suitable communication lines of host computer 1.

The loading procedure for such a system will now be described. Upon power up i.e. operatively coupling the card 3 and coupler 2, the microprocessor 4 begins to execute instructions residing in the operating system. As stated above, in the preferred system the memory portion storing the operating system is execute only and will be set upon manufacture. The data within it can be neither read nor written to by any application program. Embodiments of the invention are however envisaged in which this region is Read only. An initialisation sequence follows, an 'answer to reset' character is issued and then a loading routine begins. The card waits to receive a message to indicate that it is in communication with the loading terminal, which in this case is coupled to an host computer 1. If the card receives a suitable message before a defined time period has elapsed, an interchange of messages between host computer 1 and the card takes place and these messages are used by the card to check whether authorised software is being used within the host computer 1. Such authorisation procedures will be well known to those skilled in the art and can be used to prevent a card being programmed by means other than that defined by the card manufacturer or user. For instance, coded messages could be exchanged, and authentication or eneryption processes using shared secret keys may be implemented. If the card has been satisfied that the loader, i.e. host computer 1, is authorised, the card will clear its application memory before receiving a sequence of executable codes which are arranged to form the new application programme. This code is then stored in the application programme area 8 of the card. Finally, the software within the card is used to establish a partition between the applications program area 8 and remainder of the read/write memory region to establish a data storage area 9, in which data relevant to the intended uses of the card can be stored and altered as desired.

The partitioning can be established by any suitable means. Typically, the partition may be established by having a pointer in memory which points to each address in turn as the applications software is loaded, byte by byte. Once this software is loaded, the final byte addressed by the pointer can be stored in a register, and, when data is subsequently stored, by means of a WRITE COMMAND, this register is accessed and used to provide a suitable address, in the allowed region, which is encoded in a header transmitted with the data.

The memory areas of the card are shown in Figure 2 where one example is shown having a total memory capability of 8 k bytes. This value may of course be varied as desired. Once the partition mentioned above has been established, then the two memory regions 8 and 9 are set up, although, as shown in figure 2, the exact memory requirements may vary and be movable dependent upon the particular applications program, and memory requirements for data storage.

After the initial programming stage, the card may be removed from the terminal and will retain the applications program. When the card is subsequently powered up and does not receive a "loading" message after issuing its answer to reset, the operating system within the card directs the microprocessor to commence execution of which ever application program is held within its memory.

Should a card not be satisfied of the authenticity of a loading station, it will not load a new application program and will halt execution.

The loading function within the card can also be disabled by an applications program. Once an application program has been downloaded, debugged and tested, it is often desirable that the card's function be fixed for the remainder of its life. This can be easily achieved by a slight modification to the application program such that it calls a routine held within the operating system which serves to remove a software or hardware link, disabling the loading routine.

Claims

1. A method of loading software into a portable electronic token (1) of the type comprising processing means (4), memory means (7,8,9) and input/output means (5) and adapted for interaction with a read/write terminal (2), wherein the memory means comprises an execute only or Read only memory region (7) and a non-volatile read/write region (8,9), which method comprises operatively coupling the token and terminal, interchanging messages, under control of an operating system stored in the execute or Read only region, between the token and terminal to check whether the token and terminal are authorised, and, only if authorisation is established; loading a program code adapted to form an application program into a portion of the read/write memory region and establishing a partition between the loaded application program and the remainder of the read/write memory region, thus leaving the remainder of the read/write region free for data storage.

2. A method as claimed in claim 1 wherein control of the token is subsequently passed to the application program after appropriate authorisation is established.

3. A method as claimed in claim 1 or claim 2 wherein the token is adapted to interact with the terminal by inductive coupling and such coupling is used to load the applications software.

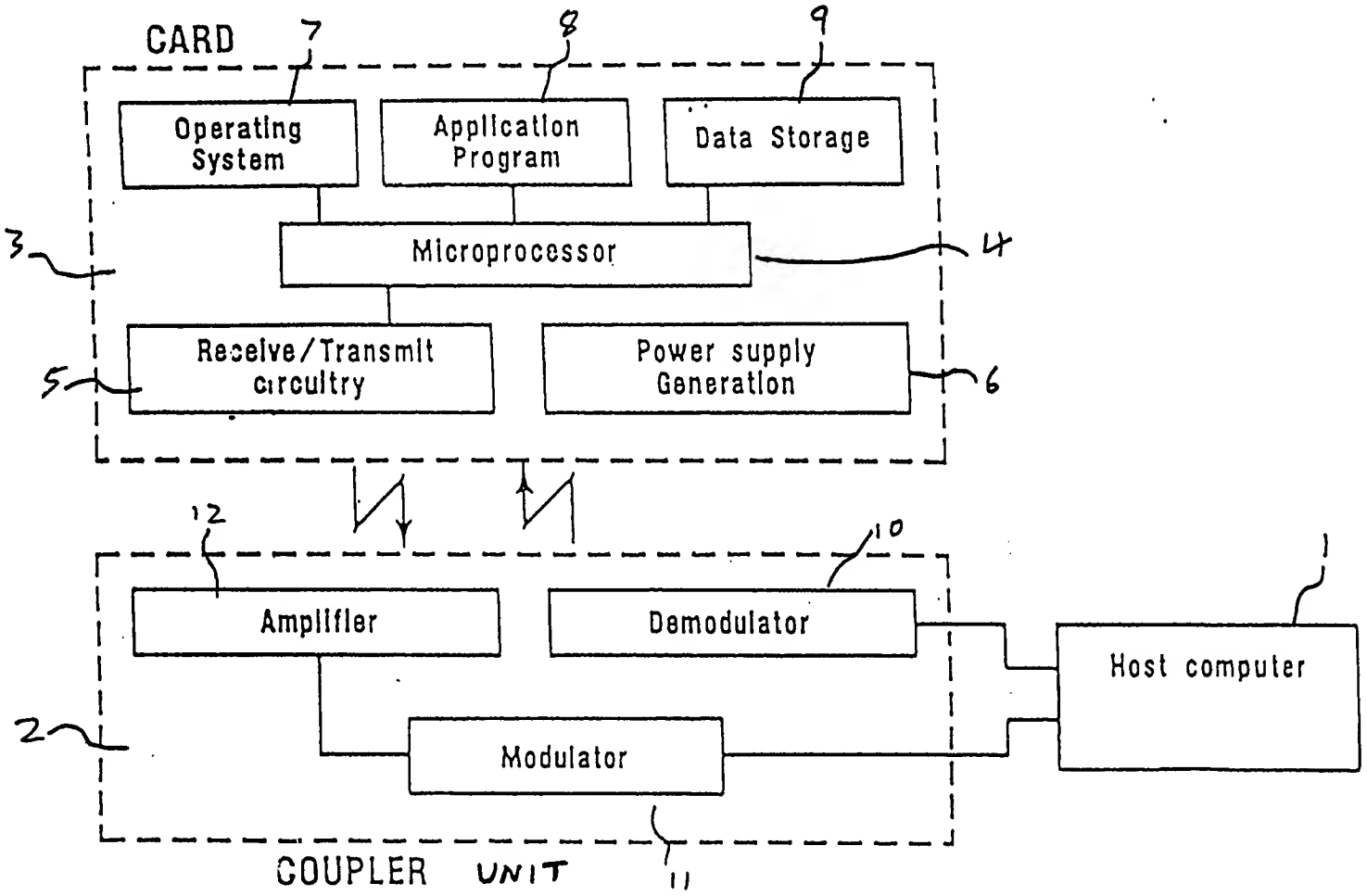
4. A method as claimed in any of the preceding claims wherein the execute only memory region includes software adapted to alter the software or hardware of the token after an applications program has been loaded such that the applications program cannot be removed or altered.

5. An electronic system comprising a port-

able electronic token (1) comprising processing means (4), memory means (7,8,9) and input/output means (5) and a read/write terminal (2) for interacting with the token, wherein the memory means comprises an execute only or Read only memory region (7) and a non-volatile read/write memory region (8,9) and wherein applications software is stored in a variable size portion (8) of the read/write region.

6. A system as claimed in claim 5 wherein the read/write region is an E^2 PROM.

7. A system as claimed in claim 5 wherein the read/write region is a battery-backed ROM.



0292248

FIGURE 1

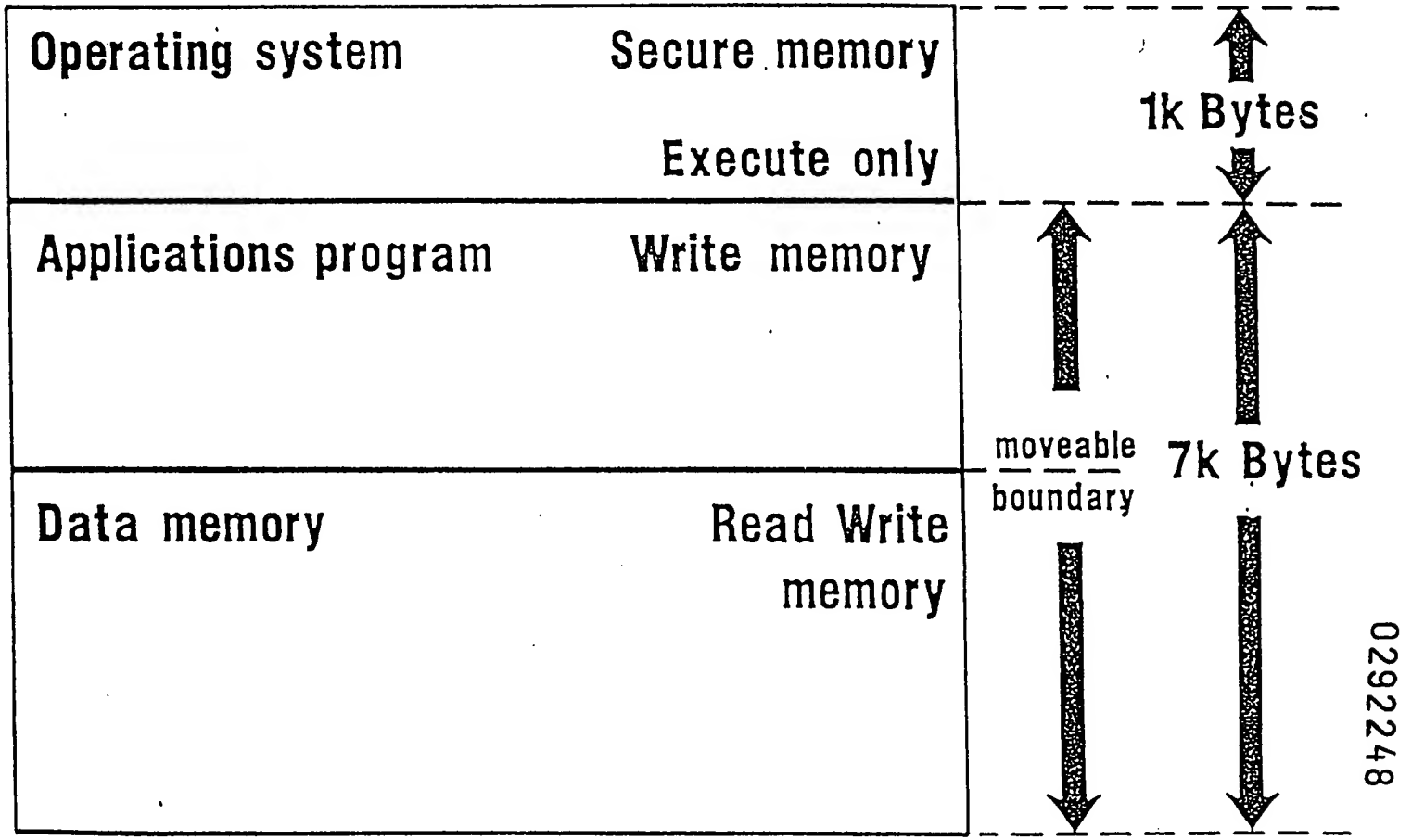

Operating system
Secure memory
Execute only
Applications program
Write memory
Data memory
Read Write memory
1k Bytes
moveable boundary
7k Bytes
0292248

FIGURE 2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 292 248**
A3

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 88304475.2

(51) Int. Cl.[5]: G07F 7/10, G07F 7/08

(22) Date of filing: 18.05.88

(30) Priority: 19.05.87 GB 8711744

(43) Date of publication of application:
23.11.88 Bulletin 88/47

(84) Designated Contracting States:
AT BE CH DE ES FR GR IT LI LU NL SE

(88) Date of deferred publication of the search report:
31.10.90 Bulletin 90/44

(71) Applicant: THE GENERAL ELECTRIC COMPANY, p.l.c.
1 Stanhope Gate
London W1A 1EH(GB)

(72) Inventor: Steiner, Anthony Francis
89 Coval Lane
Chelmsford Essex(GB)
Inventor: Edmonds, Richard
35 Coverside Road
Great Glen Leicester LE8 0EB(GB)

(74) Representative: Tolfree, Roger Keith
GEC p.l.c. Central Patent Department
Chelmsford Office Marconi Research Centre
West Hanningfield Road
Great Baddow Chelmsford Essex CM2 8HN(GB)

(54) Data processing system.

(57) The memory area within an electronic token of the 'smart card' type comprising a processor (4), memory (7, 8, 9) and input/output means (5) is divided into an execute only region and a non-volatile read/write region.

A method of loading an applications program is described in which the program is loaded into a portion of the read/write region by software methods and in which the application program may be altered if the use of the card alters.

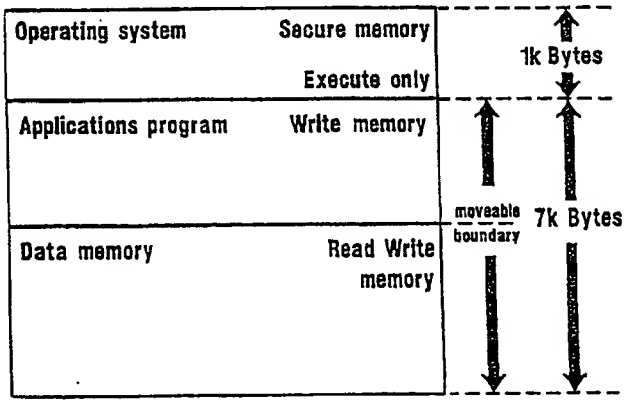


FIGURE 2

EP 0 292 248 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 88 30 4475

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.4)
A	EP-A-217654 (K.K. TOSHIBA) * the whole document *	1-7	G07F7/10 G07F7/08
A	US-A-3996449 (ATTANASIO ET.AL.) * abstract; claims 1-8; figures 1, 2c *	1, 2, 4, 5	
A	PATENT ABSTRACTS OF JAPAN vol. 11, no. 42 (P-545)(2489) 06 February 1987, & JP-A-61 211788 (HITACHI MAXELL LTD.) 19 September 1986, * the whole document *	1, 2	
A	EP-A-193920 (CASIO COMPUTER COMPANY LTD.) * the whole document *	1, 4-6	
A,P	WO-A-8707061 (AMERICAN TELEPHONE & TELEGRAPH COMPANY) * abstract; claims 1-13; figures 1-11 *	1-6	
A	EP-A-159651 (OMRON TATEISI ELECTRONICS) * abstract; claims 2-6; figure 11 *	1, 3-6	
A,D	EP-A-198642 (GENERAL ELECTRIC COMPANY) * abstract *	2-5	
A	US-A-4663707 (DAWSON) * abstract; claims 1-5 *	1-3	
A,P	WO-A-8707060 (SMART CARDS APPLICATIONS, INC.) * abstract *	1	
A	GB-A-2087606 (MASTIFF SECURITY SYSTEMS) * the whole document *	1	
A	GB-A-2168831 (STEEBEK SYSTEMS LTD.)		
A	EP-A-89876 (CII-HONEYWELL BULL)		

TECHNICAL FIELDS SEARCHED (Int. Cl.4)

G07F
G07C
G06K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	04 SEPTEMBER 1990	GUIVOL O.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)

18/5/2 (Item 2 from File: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

011215591 **Image available**
WPI Acc No: 1997-193516/199718
XRPX Acc No: N97-159806
Mutual authentication **of identified** chip cards **with computer system - involves exchange of two random numbers and use of secret OFFSET prior to reciprocal acknowledgement of agreed results of encryption**
Patent Assignee: INFORMATIKZENTRUM SPARKASSENORGANISATION (INFO-N)
Inventor: LOEHMANN E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 19523466	C1	19970403	DE 1023466	A	19950628	199718	B

Priority Applications (No Type Date): DE 1023466 A 19950628
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19523466	C1		9	H04L-009/32	

Abstract (Basic): DE 19523466 C
The **chip card** (CC) transmits an **application** (LOG) to the system (S), which returns a random number (RNS) for use with a key (K) in computing a result of encryption (V(K,RNS)). The **chip card** also determines a secret number (OFFSET) for later use and computes another result (V(K,OFFSET)). Both results are transmitted with the identifier (ID) to the system, which derives the key by an established method (F1). The first encryption result is also computed and compared with that from the **chip card** . On receipt of an acknowledgment (OK) the **chip card** sends another random number (RNC), to which the system adds the OFFSET. If the **chip card** agrees with the result, the **application** is authorised.
ADVANTAGE - Simulation of system with fraudulent intent is prevented by multiple use of common identifier.
Dwg.1/4
Title Terms: MUTUAL; AUTHENTICITY; IDENTIFY; CHIP; CARD; COMPUTER; SYSTEM; EXCHANGE; TWO; RANDOM; NUMBER; SECRET; OFFSET; PRIOR; RECIPROCAL; ACKNOWLEDGE; AGREE; RESULT; ENCRYPTION
Derwent Class: T04; W01
International Patent Class (Main): **H04L-009/32**
International Patent Class (Additional): **G06F-012/14** ; G07C-009/00
File Segment: EPI

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 195 23 466 C1**

(51) Int. Cl.[6]:
H 04 L 9/32
G 08 F 12/14
G 07 C 9/00

(21) Aktenzeichen: 195 23 466.9-31
(22) Anmeldetag: 28. 6. 95
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 3. 4. 97

DE 195 23 466 C1

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Informatikzentrum der Sparkassenorganisation GmbH, 53227 Bonn, DE

(74) Vertreter:
Patentanwälte von Kreisler, Selting, Werner et col., 50667 Köln

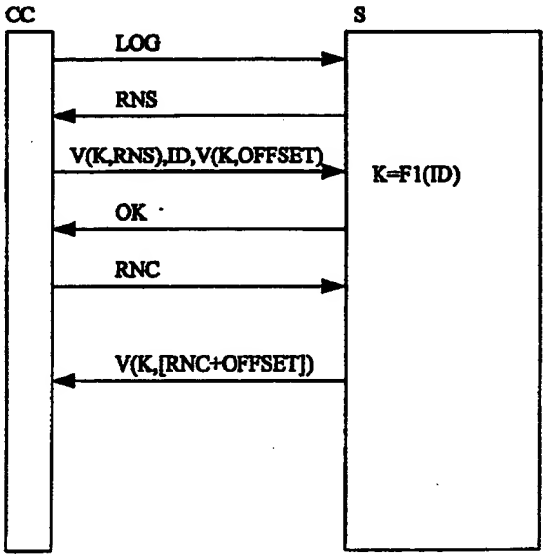
(72) Erfinder:
Löhmann, Ekkehard, 85737 Ismaning, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE	43 42 641 A1
DE	41 38 861 A1
US	52 02 921
EP	0 77 238 B1
EP	5 73 245 A2

(54) Verfahren zur gegenseitigen Authentifikation von elektronischen Partnern mit einem Rechnersystem

(57) Bei dem Verfahren zur gegenseitigen Authentifikation eines elektronischen Partners (CC) nach der "Chalenge and Response"-Methode mit einem System (S) wird zur Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC) von dem System (S) auf der Basis der von dem elektronischen Partner (CC) gelieferten zweiten Zufallszahl (RNC) und einem Geheimcode (OFFSET), der ausschließlich dem System (S) und dem elektronischen Partner (CC) bekannt ist, mittels eines Schlüssels (K) ein Verschlüsselungsergebnis errechnet, das an den elektronischen Partner (CC) zurückgesandt wird. Der elektronische Partner (CC) errechnet seinerseits auf der Grundlage ebenfalls der Zufallszahl (RNC) und dem Geheimcode (OFFSET) sowie dem Schlüssel (K) ein Verschlüsselungsergebnis. Erst dann, wenn diese beiden Verschlüsselungsergebnisse übereinstimmen, gilt das System (S) gegenüber dem elektronischen Partner (CC) als authentisch.



DE 195 23 466 C1

Beschreibung

Die Erfindung betrifft ein Verfahren zur gegenseitigen Authentifikation eines elektronischen Partners nach der "Challenge and Response" Methode mit einem System gemäß dem Oberbegriff des Anspruchs 1, wie z. B. aus DE 41 38 861 A1 bekannt.

Um Zugang zu einem System zu erhalten, muß häufig die Berechtigung zu diesem Zugang nachgewiesen werden. Andererseits muß sich auch das System eindeutig als echt zu erkennen geben, um einen möglichen Betrug durch ein simuliertes System auszuschließen. Um dies zu gewährleisten, wurde die sogenannten "Challenge and Response"-Methode entwickelt.

Bei dieser Methode schickt zunächst das System eine Zufallszahl an den elektronischen Partner. Dieser verschlüsselt diese Zufallszahl mit einem Verschlüsselungsalgorithmus sowie einem Schlüssel und sendet das Ergebnis gemeinsam mit einer Identitätskenngröße zurück an das System. Mittels eines nur dem System bekannten Verfahrens errechnet das System aus der Identitätskenngröße den Schlüssel und errechnet ebenfalls das Ergebnis, das sich mit Hilfe des Verschlüsselungsalgorithmus aus der Zufallszahl und dem Schlüssel ergibt. Stimmt das vom elektronischen Partner gesendete Ergebnis mit dem vom System errechneten überein, gilt der elektronische Partner als authentisch.

Zur Authentisierung des Systems gegenüber dem elektronischen Partner wird der oben beschriebene Vorgang mit vertauschten Rollen nochmals durchgeführt. Der elektronische Partner sendet eine Zufallszahl zum System, das System verschlüsselt diese Zufallszahl anhand des Verschlüsselungsalgorithmus und des ihm bereits bekannten Schlüssels und sendet das Ergebnis zum Vergleich an den elektronischen Partner.

Der Schlüssel ist demnach lediglich beim elektronischen Partner gespeichert, während das System diesen Schlüssel immer wieder neu nach einem nur dem System bekannten Verfahren unter Zugrundelegen der Identitätskenngröße des elektronischen Partner erzeugen muß. Diese Identitätskenngröße wird während der Initialisierungsphase (Personalisierung), d. h. vor dem erstmaligen Betrieb des Systems gemeinsam mit den elektronischen Partnern, für die elektronischen Partner festgelegt. Dabei erscheint es häufig sinnvoll, ganzen Gruppen von elektronischen Partnern die gleiche Identitätskenngröße und damit auch den gleichen Schlüssel zuzuordnen, um den elektrischen Partnern einer Gruppe die gleichen Zugriffs- und Zugangsrechte zu einem elektronischen Medium zu verleihen.

Aufgrund dieser Praxis ergibt sich aber für einen Betrüger die Möglichkeit, das System bei dessen Authentifikation gegenüber dem elektronischen Partner zu simulieren. Voraussetzung ist lediglich, daß zwei elektronische Partner mit gleicher Identitätskenngröße annähernd gleichzeitig auf das System zugreifen wollen. Die Simulation des Systems kann dann auf folgende Weise durchgeführt werden.

Das simulierende System sendet eine Zufallszahl zum ersten elektronischen Partner, dieser verschlüsselt die Zufallszahl in oben beschriebener Weise und sendet das Ergebnis gemeinsam mit der Identitätskenngröße zum simulierenden System. Dieses bestätigt die Richtigkeit des Ergebnisses, ohne es wirklich überprüft zu haben, woraufhin der erste elektronische Partner seine Zufallszahl zum simulierten System sendet. Dieses reicht die soeben empfangene Zufallszahl an einen ebenfalls gerade auf das System zugreifen wollenden zweiten elektronischen Partner weiter, der daraus — als Teil seiner Authentifikationsprozedur gegenüber dem System — in oben beschriebener Weise das benötigte Verschlüsselungsergebnis berechnet und es an das simulierte System überträgt. Das simulierte System reicht dieses Ergebnis (das mithin von einem elektronischen Partner erzeugt worden ist, der der gleichen Gruppe von Identitätskenngrößen gehört und damit über den gleichen Schlüssel verfügt) zum ersten elektronischen Partner weiter, der es mit dem selbst errechneten Ergebnis vergleicht und die Authentizität des simulierten Systems feststellt. Der zweite elektronische Partner wird durch Übertragung einer Fehlermeldung vom simulierten System abgewiesen.

In DE 41 38 861 A1 wird zwar gezeigt, wie eine Simulation des Systems in betrügerischer Absicht zu verhindern ist; dabei wird jedoch die Eingangsprämisse, nämlich, daß allen elektronischen Partner einer Gruppe die gleiche Identitätsgröße und damit der gleiche Schlüssel zugeordnet wird, durch die Einführung einer individuellen Zusatzidentitätskenngröße verletzt. Diese individuelle Zusatzidentitätskenngröße ist im elektronischen Partner fest abgespeichert.

Die der vorliegenden Erfindung zugrundeliegende Aufgabe ist es nun, bei mehrfacher Verwendung einer gemeinsamen Identitätskenngröße für mehrere elektronische Partner, die gleichzeitig an ein System angeschlossen sein können, eine Simulation des Systems in betrügerischer Absicht zu verhindern.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst, und zwar ohne Verletzung der oben genannten Prämisse. Vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind jeweils in den Unteransprüchen aufgeführt.

Nach der Erfindung wird der zusätzlich vergebene Geheimcode jedesmal erzeugt, wenn er zur Authentifikation des Systems gegenüber dem elektronischen Partner benötigt wird, wobei es grundsätzlich denkbar ist, daß bei jeder Generierung ein anderer Geheimcode entsteht. Damit kann die Eingangsprämisse, daß eine Gruppe elektronischer Partner mit gleicher Zugriffs- bzw. Zugangsberechtigung mit Ausnahme der Identitätskenngröße keine weiteren Individualisierungskenndaten, insbesondere keine die elektronischen Partner dieser Gruppe untereinander unterscheidenden Individualisierungskenndaten aufweisen, beibehalten werden. Erfindungsgemäß wird der Geheimcode mit der vom elektronischen Partner übermittelten Geheimzahl mathematisch verknüpft. Dabei stellt der Geheimcode ein Geheimnis dar, das lediglich einem elektronischen Partner und nach Versendung dem System bekannt ist.

Durch die erfindungsgemäße Erweiterung des Challenge Response Protokolls kann in vorteilhafter Weise für jeden einzelnen elektronischen Partner ein Austausch von Zufallszahlen mit dem System erreicht werden, so daß danach zweifelsfrei sowohl die Identität des elektronischen Partners als auch die Identität des Systems feststeht, ohne daß dies durch die quasi zeitgleiche Anmeldung eines weitern elektronischen Partners gefährdet wäre.

Damit kann im Falle der Zusammenfassung von elektronischen Partnern in Gruppen mit identischen Identitätskenngrößen einer betrügerischen Simulation des Systems gegenüber einem elektronischen Partner erfolgreich begegnet werden.

Nachfolgend werden anhand der Zeichnung Ausführungsbeispiele der Erfindung näher erläutert. Im einzel-

nen zeigen:

Fig. 1 bis 3 alternative Ausführungsbeispiele des erfindungsgemäßen Verfahrens und

Fig. 4 den Verfahrensablauf bei simuliertem System.

Im folgenden wird anstelle des Begriffes "elektronischer Partner", der für ein beliebig ausgeformtes elektronisches Gerät mit den Fähigkeiten einer Chipkarte steht, der Begriff "Chipkarte" verwendet.

Am linken Rand der Fig. 4 ist symbolisch eine erste Chipkarte CC1 und am rechten Rand symbolisch eine zweite Chipkarte CC2 gezeigt. Zwischen den beiden Chipkarten CC1, CC2 ist symbolisiert durch ein Rechteck ein simuliertes System SS abgebildet. Zu einem bestimmten Zeitpunkt wird beispielsweise durch Einstekken der ersten Chipkarte CC1 in ein Kartenlesegerät die erste Chipkarte CC1 mit dem simulierten System SS verbunden. Die erste Chipkarte CC1 überträgt an das simulierte System SS eine Anmeldeinformation LOG. Daraufhin überträgt das simulierte System SS eine erste Zufallszahl RNS zur ersten Chipkarte CC1. Diese verschlüsselt anhand des Verschlüsselungsalgorithmus V und des in der Karte gespeicherten Schlüssels K die erste Zufallszahl RNS. Das Verschlüsselungsergebnis V (K, RNS) und die in der ersten Chipkarte CC1 gespeicherte Identitätsnummer ID werden zum simulierten System SS übertragen. Das simulierte System SS überträgt ein Quittungssignal OK an die erste Chipkarte CC1. Die erste Chipkarte CC1 interpretiert das Quittungssignal OK so, als wäre der Authentifizierungsprozeß der ersten Chipkarte CC1 gegenüber dem simulierten System SS erfolgreich verlaufen. Deshalb sendet die erste Chipkarte CC1 zur Authentizitätsprüfung des simulierten Systems SS eine zweite Zufallszahl RNC zum simulierten System SS.

Wird nun gleichzeitig oder annähernd gleichzeitig eine zweite Chipkarte CC2, beispielsweise durch Einschieben in ein weiteres Kartenlesegerät mit dem simulierten System SS verbunden, so ergibt sich für den Fall, daß die zweite Chipkarte CC2 die gleiche Identitätskenngröße ID wie die erste Chipkarte CC1 hat die folgende Situation: Zunächst meldet sich auch die zweite Chipkarte CC2 durch Übertragen einer Anmeldeinformation LOG beim simulierten System SS an. Das simulierte System SS reicht nun die von der ersten Chipkarte CC1 empfangene zweite Zufallszahl RNC an die zweite Chipkarte CC2 weiter. Die zweite Chipkarte CC2 verschlüsselt die durchgereichte Zufallszahl RNC mit Hilfe des Verschlüsselungsalgorithmus V und des Schlüssels K und gibt das Verschlüsselungsergebnis V (K, RNC) und die Identitätsnummer ID zum simulierten System SS. zurück. Das simulierte System SS verfügt nun über das zur Authentifikation gegenüber der ersten Chipkarte CC1 erforderliche Verschlüsselungsergebnis V (K, RNC) und überträgt dieses zur ersten Chipkarte CC1. Die gegenseitige Authentifikation zwischen erster Chipkarte CC1 und simuliertem System SS ist damit erfolgreich abgeschlossen. Die zweite Chipkarte CC2 erhält ein negatives Quittungssignal F und wird damit abgewiesen.

In Fig. 1 bis 3 wird nun aufgezeigt, wie die oben beschriebene Authentifikation eines simulierten und damit unberechtigten Systems SS gegenüber einer Chipkarte CC wirksam verhindert werden kann.

Dazu wird das Protokoll so abgeändert, daß bei der Authentifikation des Systems S gegenüber dem elektronischen Partner CC ein zusätzlicher Geheimcode OFFSET (nachfolgend auch geheime Zahl genannt), der dem elektronischen Partner CC zum Zeitpunkt der Initialisierung und dem System S zum Zeitpunkt der Authentifikation bekannt ist, verwendet werden kann. Der Geheimcode OFFSET ist jedoch für alle elektronischen Partner mit derselben Identitätskenngröße gleich.

Auf die Challenge des elektronischen Partners CC (Senden der Zufallszahl RNC) reagiert das System durch Senden des verschlüsselten Wertes von RNC plus OFFSET.

Der relevante Geheimcode OFFSET wird entweder dem System S vom elektronischen Partner als Teil seiner Response auf die Challenge des System (siehe Fig. 1) oder in einem zusätzlichen Protokollschritt verschlüsselt übermittelt, der zwischen der Authentifikation des elektronischen Partners CC und der Authentifikation des Systems liegt, dem System verschlüsselt vom elektronischen Partner CC übermittelt (siehe Fig. 2) oder der die geheime Zahl OFFSET wird bereits zum Zeitpunkt der Initialisierung mit einem geheimen Verfahren F2 aus der Identitätskenngröße ID berechnet und analog zum Schlüssel K beim elektronischen Partner CC gespeichert, wobei der Geheimcode OFFSET im Zuge der Authentifikation des Systems S vom System S aus der übermittelten Identitätsgröße mittels des geheimen Verfahrens F2 jeweils neu berechnet wird (siehe Fig. 3).

Die gegenseitige Authentifikation zwischen Chipkarte CC und System S verläuft dann in Fig. 1 wie folgt:
Die Chipkarte CC überträgt eine Anmeldeinformation LOG an das System S. Das System S erzeugt eine Zufallszahl RNS und überträgt diese an die Chipkarte CC. Die Chipkarte errechnet aus dem Schlüssel K und der Zufallszahl RNS ein Verschlüsselungsergebnis V (K, RNS). Außerdem bestimmt die Chipkarte den später zu verwendenden OFFSET und errechnet aus dem Schlüssel K und der geheimen Zahl OFFSET das Verschlüsselungsergebnis V (K, OFFSET). Gemeinsam mit der Identitätskenngröße ID werden diese beiden Werte zum System S übertragen. Das System S errechnet aus der Identitätskenngröße ID mit Hilfe des festgelegten Verfahrens F1 den Schlüssel K. Das System S berechnet ebenfalls das Verschlüsselungsergebnis V (K, RNS) und vergleicht es mit dem in der Chipkarte errechneten und zum System S übertragenen Verschlüsselungsergebnis V (K, RNS). Bei positivem Vergleichsergebnis überträgt das System S ein positives Quittungssignal OK an die Chipkarte CC. Außerdem bestimmt das System mit Hilfe von K die geheime Zahl OFFSET. Nach Empfang des Quittungssignals OK sendet die Chipkarte CC eine Zufallszahl RNC zum System S. Das System S addiert zu dieser Zufallszahl RNC den Wert des OFFSET und verschlüsselt das Ergebnis der Addition. Das Verschlüsselungsergebnis V (K, [RNC+OFFSET]) wird zur Chipkarte CC übertragen und dort analog überprüft. Bei positivem Vergleichsergebnis sendet die Chipkarte CC ein positives Quittungssignal OK zum System S. Die gewünschte Anwendung ist damit freigegeben.

Die gegenseitige Authentifikation zwischen Chipkarte CC und System S verläuft dann in Fig. 2 wie folgt:
Die Chipkarte CC überträgt eine Anmeldeinformation LOG an das System S. Das System S erzeugt eine Zufallszahl RNS und überträgt diese an die Chipkarte CC. Die Chipkarte errechnet aus dem Schlüssel K und der Zufallszahl RNS ein Verschlüsselungsergebnis V (K, RNS). Außerdem bestimmt die Chipkarte den später zu verwendenden Geheimcode OFFSET und errechnet aus dem Schlüssel K und dem Geheimcode OFFSET das Verschlüsselungsergebnis V (K, OFFSET).

Das Verschlüsselungsergebnis V(K, RNS) wird zu-

sammen mit der Identitätskenngröße zum System S übertragen. Das System S errechnet aus der Identitätskenngröße ID mit Hilfe des festgelegten Verfahrens F1 den Schlüssel K. Das System S berechnet ebenfalls das Verschlüsselungsergebnis V (K, RNS) und vergleicht es mit dem in der Chipkarte errechneten und zum System S übertragenen Verschlüsselungsergebnis V (K, RNS). Bei positivem Vergleichsergebnis überträgt das System S ein positives Quittungssignal OK an die Chipkarte CC. Daraufhin überträgt die Chipkarte CC das schon berechnete Verschlüsselungsergebnis V(K, OFFSET) zusammen mit der Identitätsgröße ID. Das System quittiert wieder mit OK. Nach Empfang des zweiten Quittungssignals OK sendet die Chipkarte CC eine Zufallszahl RNC zum System S. Das System S addiert zu dieser Zufallszahl RNC den Wert der geheimen Zahl OFFSET, den das System aus dem empfangenen Wert V(K, OFFSET) berechnet hat und verschlüsselt das Ergebnis der Addition. Das Verschlüsselungsergebnis V (K, [RNC+OFFSET]) wird zur Chipkarte CC übertragen und dort analog überprüft. Bei positivem Vergleichsergebnis sendet die Chipkarte CC ein positives Quittungssignal OK zum System S. Die gewünschte Anwendung ist damit freigegeben.

In Fig. 3 wird davon ausgegangen, daß der Geheimcode OFFSET bereits zum Zeitpunkt der Initialisierung mit einem geheimen Verfahren F2 aus der Identitätskenngröße ID berechnet und analog zum Schlüssel K beim elektronischen Partner CC gespeichert wurde.

Die gegenseitige Authentifikation zwischen Chipkarte CC und System S verläuft dann in Fig. 3 wie folgt:
Die Chipkarte CC überträgt eine Anmeldeinformation LOG an das System S. Das System S erzeugt eine Zufallszahl RNS und überträgt diese Chipkarte CC. Die Chipkarte errechnet aus dem Schlüssel K und der Zufallszahl RNS ein Verschlüsselungsergebnis V (K, RNS) welches zusammen mit der Identitätskenngröße ID zum System S übertragen. Das System S errechnet aus der Identitätskenngröße ID mit Hilfe des festgelegten Verfahrens F1 den Schlüssel K. Das System S berechnet ebenfalls das Verschlüsselungsergebnis V (K, RNS) und vergleicht es mit dem in der Chipkarte errechneten und zum System S übertragenen Verschlüsselungsergebnis V (K, RNS). Bei positivem Vergleichsergebnis überträgt das System S ein positives Quittungssignal OK an die Chipkarte CC.

Nach Empfang des Quittungssignals OK sendet die Chipkarte CC eine Zufallszahl RNC zum System S.

Das System berechnet aus der vorher übertragenen Identitätsgröße ID und aus dem geheimen Verfahren F2 den Geheimcode OFFSET, addiert diesen Wert zur empfangenen Zufallszahl RNC und verschlüsselt das Ergebnis der Addition. Das Verschlüsselungsergebnis V (K, [RNC+ OFFSET]) wird zur Chipkarte CC übertragen. Die Chipkarte CC addiert zur gesendeten Zufallszahl RNC den in der Chipkarte gespeicherten Geheimcode OFFSET und führt die Verschlüsselung dieser Addition mit dem Schlüssel K durch und vergleicht das Ergebnis mit dem vom System S empfangenen Wert V(K, [RNC+OFFSET]). Bei positivem Vergleichsergebnis sendet die Chipkarte CC ein positives Quittungssignal OK zum System S. Die gewünschte Anwendung ist damit freigegeben.

Patentansprüche

1. Verfahren zur gegenseitigen Authentifikation eines eine Identitätskenngröße aufweisenden elektronischen Partners und eines Systems, auf das eine Vielzahl von elektronischen Partnern zugreifen darf, von denen jeweils mehrere gleichberechtigt in Gruppen mit gleicher Identitätskenngröße zusammengefaßt sind,

— bei dem zur Authentifikation des elektronischen Partners (CC) gegenüber dem System (S)

— das System (S) eine erste Zufallszahl (RNS) an den elektronischen Partner (CC) sendet,

— der elektronische Partner (CC) die erste Zufallszahl (RNS) mittels eines Schlüssels (K) verschlüsselt und das Verschlüsselungsergebnis zusammen mit der Identitätskenngröße (ID) an das System (S) zurücksendet,

— das System (S) zunächst anhand der Identitätskenngröße (ID) den Schlüssel (K) ermittelt und anschließend mittels dieses Schlüssels (K) aus der ersten Zufallszahl (RNS) ein Verschlüsselungsergebnis errechnet,

— das System das vom elektronischen Partner (CC) erhaltene Verschlüsselungsergebnis und das selbst errechnete Verschlüsselungsergebnis vergleicht, wobei bei Gleichheit beider Verschlüsselungsergebnisse der elektronische Partner (CC) gegenüber dem System (S) als authentisch gilt,

— und bei dem zur Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC)

— der elektronische Partner (CC) eine zweite Zufallszahl (RNC) an das System (S) sendet,

— das System (S) die zweite Zufallszahl (RNC) mittels des anhand der Identitätskenngröße (ID) des elektronischen Partners (CC) ermittelten Schlüssels (K) verschlüsselt und das Verschlüsselungsergebnis an den elektronischen Partner (CC) sendet,

— der elektronische Partner (CC) anhand der zweiten Zufallszahl (RNC) und des Schlüssels (K) ein Verschlüsselungsergebnis errechnet und

— der elektronische Partner (CC) das von dem System (S) erhaltene Verschlüsselungsergebnis und das selbst errechnete Verschlüsselungsergebnis vergleicht, wobei bei Gleichheit beider Verschlüsselungsergebnisse das System (S) gegenüber dem elektronischen Partner (CC) als authentisch gilt,

dadurch gekennzeichnet,

— daß bei der Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC)

— das System (S) sein Verschlüsselungsergebnis auf der Basis eines lediglich dem System (S) und dem elektronischen Partner (CC) bekannten erzeugten Geheimcodes (OFFSET) und der vom elektronischen Partner (CC) erhaltenen zweiten Zufallszahl (RNC) mittels des Schlüssels (K) errechnet und an den elektronischen

Partner (CC) sendet, wobei der Geheimcode (OFFSET) mit der vom elektronischen Partner (CC) gesendeten zweiten Zufallszahl (RNC) in dem System (S) mathematisch verknüpft wird,

— der elektronische Partner (CC) sein Verschlüsselungsergebnis auf der Basis des Geheimcodes (OFFSET) und der zweiten Zufallszahl (RNC) errechnet und

— der elektronische Partner (CC) das von dem System (S) erhaltene Verschlüsselungsergebnis mit dem selbst errechneten Verschlüsselungsergebnis vergleicht, wobei bei Gleichheit beider Verschlüsselungsergebnisse das System (S) gegenüber dem elektronischen Partner (CC) als authentisch gilt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) dem System (S) insbesondere in mittels des Schlüssels (K) verschlüsselter Form bei der Authentifikation des elektronischen Partners (CC) gegenüber dem System (S) übermittelt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) dem System (S) insbesondere in mittels des Schlüssels (K) verschlüsselter Form nach der Authentifikation des elektronischen Partners (CC) gegenüber dem System (S) übermittelt wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) zum Zeitpunkt der Initialisierung des elektronischen Partners (CC) aus dessen Identitätskenngröße (ID) berechnet und im elektronischen Partner (CC) gespeichert wird und daß der Geheimcode (OFFSET) für die Authentifikation des Systems (S) gegenüber dem elektronischen Partner (CC) aus dessen Identitätskenngröße (ID) neu berechnet wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) zu der vom elektronischen Partner (CC) gesendeten zweiten Zufallszahl (RNC) in dem System (S) hinzuaddiert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß der Geheimcode (OFFSET) durch einen Zufallsgenerator erzeugt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß der elektronische Partner (CC) eine Chipkarte ist.

Hierzu 4 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 195 23 466 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

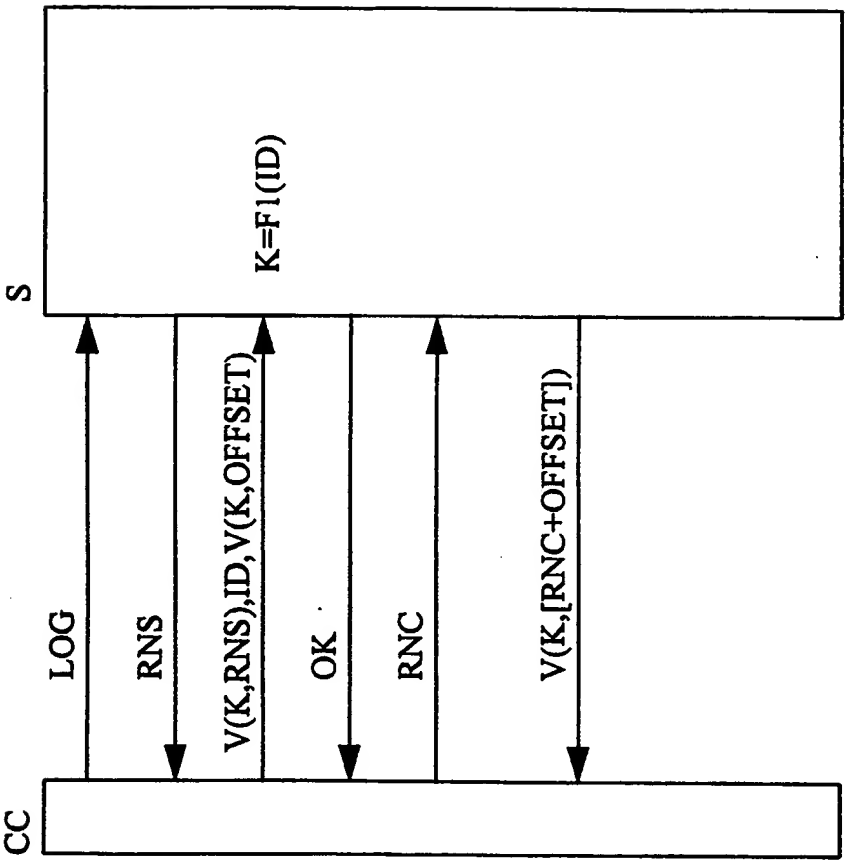


FIG 1

Nummer: DE 195 23 466 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

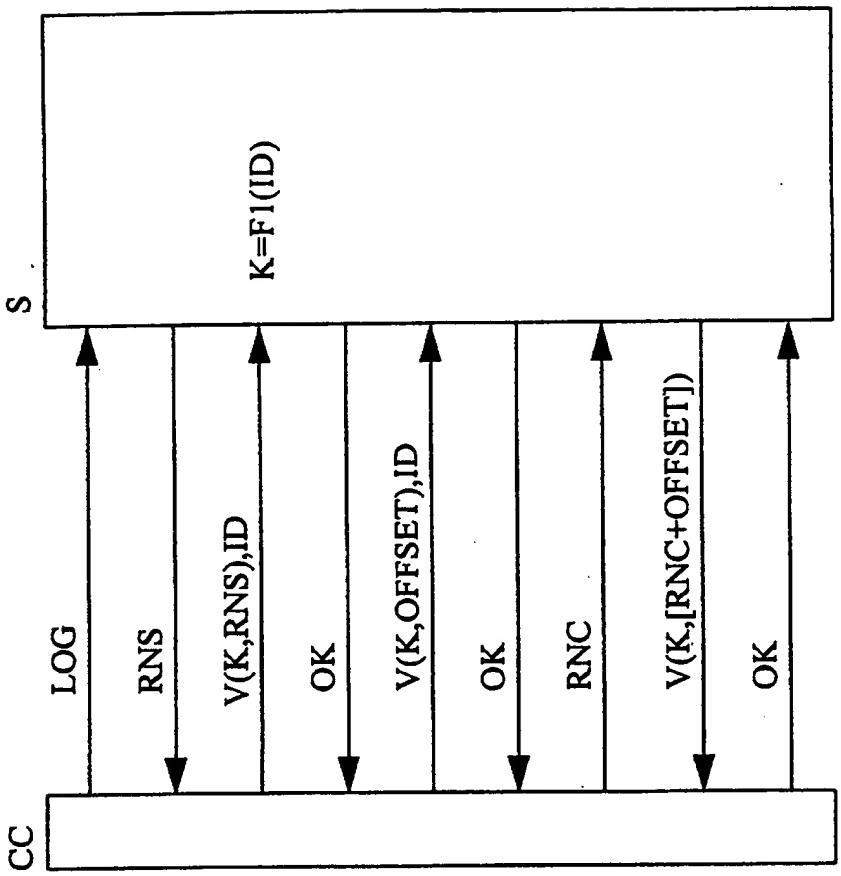


FIG 2

Nummer: DE 195 23 468 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

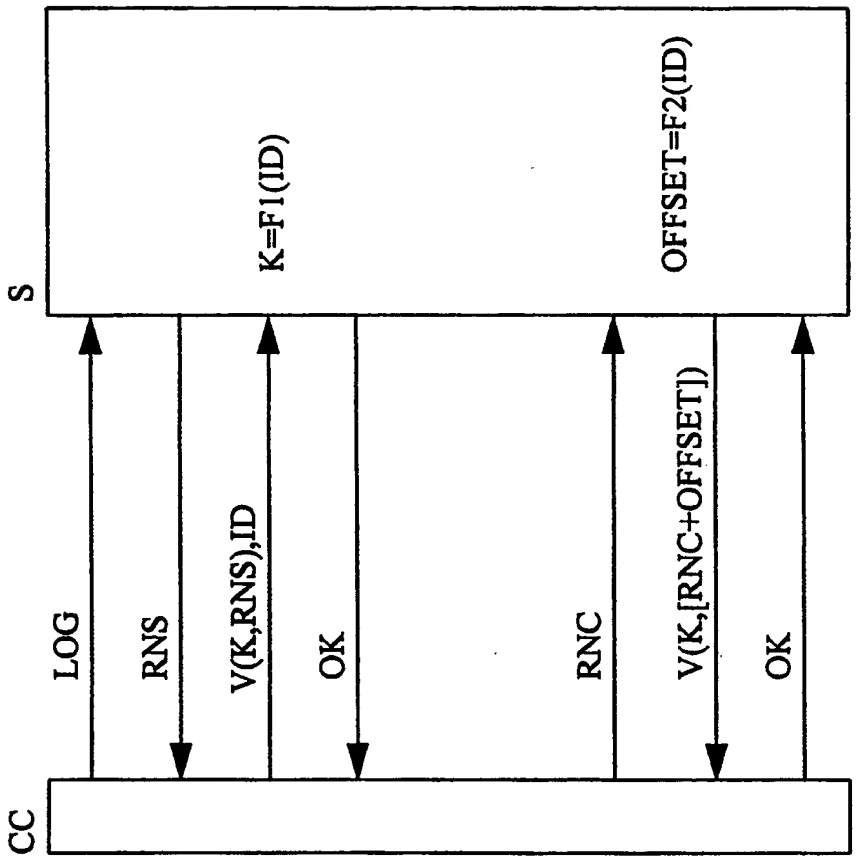


FIG 3

Nummer: DE 195 23 466 C1
Int. Cl.[6]: H 04 L 9/32
Veröffentlichungstag: 3. April 1997

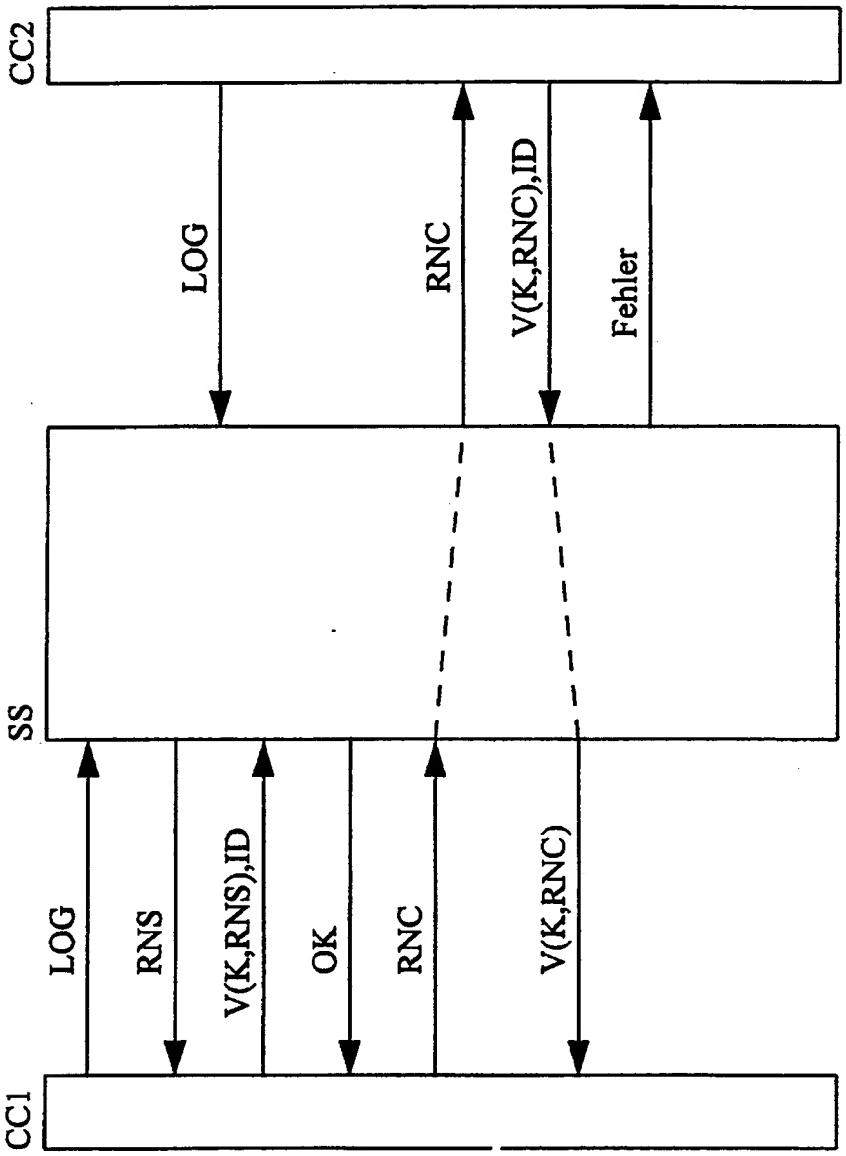


FIG 4

19/5/5 (Item 5 from File: 347)
DIALOG(R)File 347:JAPIO

05650716 **Image available**
PROCESSOR FOR PREPAID IC CARD

PUB. NO.: 09-265516 [JP 9265516 A]
PUBLISHED: October 07, 1997 (19971007)
INVENTOR(s): NISHIOKA MITSURU
APPLICANT(s): TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-076201 [JP 9676201]
FILED: March 29, 1996 (19960329)
INTL CLASS: [6] G06K-017/00; A63F-007/02; G07F-007/08; G07F-007/12
JAPIO CLASS: 45.3 (INFORMATION PROCESSING -- Input Output Units); 29.4 (PRECISION INSTRUMENTS -- Business Machines); 30.2 (MISCELLANEOUS GOODS -- Sports & Recreation)

ABSTRACT

PROBLEM TO BE SOLVED: To prevent a secret key, etc., from being leaked, or stolen and illegally used, or illegal use through an alteration of a subtracting machine, etc., by registering collation data from a **2nd** IC **card** in a handling means, and judging the propriety of a 1st IC card which has operation data enabling normal operation on the basis of the collation data.

SOLUTION: An operator inserts a registration card into equipment. When the inserted card is a registered and 'rewriting' is permitted by setting and data are not registered, the equipment side perform **mutual authentication** for confirming the propriety of the card. When the result is OK, an inputted password code is matched so as to confirm the propriety of the user, and then the registered data beings to be read for the 1st time after OK is obtained. When the password number is NG, data are not outputted even if a read of the data from the card is tried. The data which are thus read out are stored in the memory in the equipment and used for subsequent equipment operation. After it is confirmed that the data are normally recorded in the memory, the card is ejected.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－265516

(43)公開日　平成９年(1997)10月７日

(51)Int.Cl.*	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｓ	
				Ｂ	
				Ｒ	
Ａ６３Ｆ　7/02	３３４		Ａ６３Ｆ　7/02	３３４	
Ｇ０７Ｆ　7/08			Ｇ０７Ｆ　7/08	Ｌ	

審査請求　未請求　請求項の数13　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平8－76201

(22)出願日　平成８年(1996)３月29日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　西岡　満
神奈川県川崎市幸区柳町70番地　東芝インテリジェントテクノロジ株式会社内

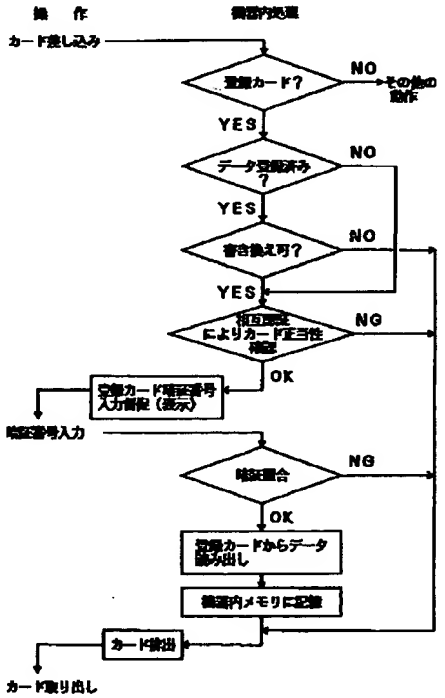
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　プリペイド用ＩＣカード処理装置

(57)【要約】

【課題】　ＩＣカードをプリペイドカード等として使用する場合の秘密鍵等の漏洩、盗難・不正使用等に関する問題を解決するＩＣカード処理システムを提供する。

【解決手段】　ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い装置と、前記取扱い装置の通常動作を可能とする動作データ、及び前記取扱い装置との間で相互に認証するための第１の相互認証プログラムを有する第１のＩＣカードと、前記取扱い装置が前記第１のＩＣカードとの間で相互に認証するための第２相互認証プログラムを有する第２のＩＣカードを具備する。



1

【特許請求の範囲】

【請求項1】　ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、
前記取扱い手段の通常動作を可能とする動作データを有する第1のＩＣカードと、
前記取扱い手段が前記第1のＩＣカードを照合するための照合データを有する第2のＩＣカードを具備し、
前記第2のＩＣカードから前記照合データが前記取扱い手段に登録され、登録された照合データを基に前記第1のＩＣカードの正当性が判断されることを特徴とするＩＣカード処理システム。

【請求項2】　ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、
前記取扱い手段の通常動作を可能とする動作データ、及び前記取扱い手段との間で相互に認証するための第1の相互認証プログラムを有する第1のＩＣカードと、
前記取扱い手段が前記第1のＩＣカードとの間で相互に認証するための第2相互認証プログラムを有する第2のＩＣカードを具備し、
前記第2のＩＣカードから前記第2の相互認証プログラムが前記取扱い手段に登録され、登録された前記第2の相互認証プログラム及び前記第1のＩＣカードが有する前記第1の相互認証プログラムを基に、前記第1のＩＣカード及び前記取扱い手段は互いに認証を確認しあうことを特徴とするＩＣカード処理システム。

【請求項3】　前記取扱い手段は、前記第1のＩＣカードにより登録されたデータを、登録から一定時間後に自動的に消去する手段を更に有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項4】　前記取扱い手段は、前記第1のＩＣカードにより登録されたたデータを、毎日一定時刻に自動的に消去する手段を更に有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項5】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記格納手段に格納された前記動作データを消去する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項6】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項7】　前記取扱い手段は、光センサにより前記蓋が開いたことを検出する手段を有することを特徴とする請求項5又は6記載のＩＣカード処理システム。

【請求項8】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記

2

取扱い手段の筐体が破壊されたことを検出して前記格納手段に格納された前記動作データを消去する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項9】　前記取扱い手段は、前記第1のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が破壊されたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有することを特徴とする請求項1又は2記載のＩＣカード処理システム。

【請求項10】　前記取扱い手段は、前記筐体部材内に張り巡らせた回路網が断たれることにより筐体の破壊を検出する手段を有することを特徴とする請求項8又は9記載のＩＣカード処理システム。

【請求項11】　前記取扱い手段は、ＩＣカードとの間で正当性確認情報を付加した電文を送受信することにより、前記ＩＣカードの正当性を確認する手段を有することを特徴とする請求項1～10のいずれか一項に記載のＩＣカード処理システム。

【請求項12】　前記取扱い手段は、複数の要因でＩＣカードの正当性を判断し、その判断結果により単なる不適合カードか偽造された不正カードかを判断する手段を有することを特徴とする請求項1～11のいずれか一項に記載のＩＣカード処理システム。

【請求項13】　前記取扱い手段は、不適合カードは排出し、不正カードは内部に取り込むかそのまま保持したまま他の機器へ発報する手段を有することを特徴とする請求項12記載のＩＣカード処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はＩＣカードを扱う装置に関し、特にプリペイドカード等の一部金額情報を書き換えて繰り返し使用できるＩＣカードを扱う機器における方式及び構造等に関する。

【0002】

【従来の技術】現在多くのプリペイドカードは、ある金額の価値付けがされたカードを購入し、その額面だけ使い切ったらカード自体廃棄する使い切りタイプだが、一部金額情報を書き換えて繰り返し使用できるものもある。

【0003】ＩＣカードをプリペイドカードとして使用する場合、機器におけるカード内の金額操作には増額（加算）と減額（減算）があり、加算を実行する機器は入金機として特別の扱いを受ける。即ち、自動式の場合、投入された現金に応じた金額をカードに書き込み内部に現金が蓄積される。又、係員等が現金を受け取り手操作により、支払われた現金に応じた金額をカードに書き込むため、厳格な操作資格管理が必要となる。従来、このような機器は次に示すような動作を行っている。

【0004】（1．1）　秘密鍵等はメーカでプログラ

ムメモリに記録

ＩＣカードを扱う機器では、相互認証やデータの暗号化等に使用する暗号・復号化論理をプログラム化して機器内のＲＯＭ等のプログラムメモリに記録している。この様なデータはメーカでの機器製造時に記録されることになる。又ＩＣカードを扱う機器では、相互認証やデータの暗号化等に使用する秘密鍵をカードと相互に持ち合う場合が多い。この秘密鍵も、機器側のプログラムで扱われるため、機器内のＲＯＭ等のプログラムメモリに記録されている。

【０００５】（１．２）　カード販売機は電源とカードがあれば動作する

プリペイドカードの販売機としては、価値付け済みのカードを内部に蓄えておき「もの」として額面金額で販売するものと、価値付けしていないカードを内部に蓄えておき、投入金額に応じて都度価値付けして販売するものがある。又再度価値付け（増額）して再利用する運用形態の場合、単なる販売機ではなくカードへの入金機となるが、いずれも動作に必要な条件は「電源が供給されること」と「カードが供給されること」である。

【０００６】（１．３）　プリペイド残額の減算＝金額情報の書き換え

プリペイドカードにより物品を購入したりサービスを受けた際、物品の価額やサービスに応じた代価の支払いにあたる残額の減算は、カードに記録された金額情報をそれまでの値から、より小さい値（又は少ない金額、量を表す情報）への「書き換え」である。

【０００７】（１．４）　形状チェックと記録データ内容の照合により不適合カードを検出

機器に差し込まれたカードに対して、形状・電気特性等の物理的事項とカードに記録されているデータの照合により適合するカードがどうかが確認される。尚、実際には形状が違えば搬送・保持機構が正常に動作できないため、そのカードは受け付けられない。又、照合用の（キー）データに限らず、読出したデータの形式や値の範囲が規定外であった場合、処理を継続できないため、結果的に不整合カードを検出したことになる。このように、従来は積極的に不適合条件を検査するわけではない。

【０００８】（１．５）　不適合カードは排出する

差し込まれたカードに対して上記のような、物理的、論理的不適合が検出された場合、機器は単純に「使用できない」としてカードを受け付けずに排出する。

【０００９】

【発明が解決しようとする課題】ＩＣカードをプリペイドカードとして扱う従来の機器は次に示すような課題を有している。

（２．１）　秘密鍵等の漏洩

ＩＣカードを扱う機器では、相互認証やデータの暗号化等に使用する暗号・復号化プログラムやＩＣカードと相互に持ち合う秘密鍵は、機器内のＲＯＭ等のプログラムメモリに記録されているため、機器の筐体を開いてプログラムメモリの内容を読出すことでこれらを入手することができる。又、これらの暗号・復号化プログラムや秘密鍵はメーカでの機器製造時にプログラムメモリに書き込まれるか、又はメーカでは機器ハードのみ製造しプリペイドシステムの管理会社において別に作成したプログラムＲＯＭを機器へ実装する等の手順があるが、基本的にエンドユーザの手に渡る前に動作可能な状態となるため、輸送途中で盗難されたり、倉庫等に保管している間に、次のような手段でプログラムメモリの内容を読出すことができる。

【００１０】具体的読出し方法として、プログラムや秘密鍵情報がＲＯＭに格納されているならば、このＲＯＭを取り外して市販のＲＯＭライタでダンプすることができる。又、制御回路にＩＣＥ(In Circuit Emulator) を接続すれば、上記のＲＯＭの内容は勿論、その他のメモリ素子等に記録されている内容でも自由に読出すことができる。

【００１１】これらの情報が入手できれば、同機能の機器やカードを偽造することができる。尚、秘密鍵については生データではなく、暗号化等が施された状態で機器のメモリに格納することが考えられるが、その機器の処理動作の一つとして秘密鍵を生データに戻す復号化が必ず存在するため、前述のＩＣＥを接続してプログラムを動作させればカードとのやりとりの経過処理において秘密鍵の値を得ることができる。この様な問題は、通信路を媒介として遠隔で相互に認証したりデータを秘匿化して交換するようなシステムで使用する機器においても内在している。

【００１２】（２．２）盗難・不正使用

プリペイドカードの販売機として、価値付け済みのカードを「もの」として額面金額で販売するものについては、販売機ごと盗まれても被害は内部に蓄えているカード（及び販売時投入された現金）だけだが、価値付けされていないカードを投入金額に応じて都度価値付けして販売するものや、カードを再利用する運用形態で入金機として機能するものの場合、カードが手に入ればその販売機を使用することで正当な代価を支払うことなく自由な金額で価値付けされたカードを作成することができる。

【００１３】（２．３）減算機の改造による不正使用

プリペイドカードによる物品の価額やサービスに応じた代価の支払いにあたる残額の減算は、カードに記録された金額情報の「書き換え」であるため、減算機能を持った機器（以下減算器）を改造することで前述の価値付けされていないカードが手に入れば前述同様に正当な代価を支払うことなく、自由な金額で価値付けされたカードを作成することができる。

【００１４】減算機は例えば無人稼動するものとしてはカード式電話機や飲料の自動販売機等があり、有人で人

5

手で操作するものとしてはＰＯＳレジ等に接続する汎用のプリペイドカード処理機等があるが、前者の場合やや大型ではあるが無人であり、後者の場合有人ではあるが小型なのでいずれも盗難の危険性は高いといえる。

【００１５】なお、上記の価値付けされていないカードを投入金額に応じて都度価値付けして販売するカード販機売機は、上記の様な不正使用方法が明確なため一般的に強固な盗難防止策がとられる。もちろん減算についても上記のような危険を内在していることが明確だが、市中での運用上販売機と同寺の盗難対策は困難といえる。

【００１６】（２．４）　不適合カードめ検査方法

従来は、差し込まれたカードに対して積極的に不適合条件を検査するわけではなく、形状・電気特性等の物理的事項とカードに記録されているデータの照合により適合するカートかどうかを確認しているに過ぎないため、たとえ高セキュリティのＩＣカードを使用したとしても偽造の危険性はまだ高いレベルにあるといえる。

【００１７】（２．５）　不正カード使用対策

従来、差し込まれたカードが不適合の場合、機器は単純に「使用できない」として受け付けずにカードを排出するだけなので、実際に偽造カード使用等の不正があつた場合にも、その使用者の特定やカードの回収はできない。

【００１８】従って本発明の目的は、ＩＣカードをプリペイドカード等として使用する場合の前述した秘密鍵等の漏洩、盗難・不正使用、減算機の改造による不正使用、不適合カードめ検査方法、不正カード使用対策に関する課題を解決するＩＣカード処理システムを提供することである。

【００１９】

【課題を解決するための手段】上記課題を解決するために本発明による第１のＩＣカード処理システムは、ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、前記取扱い手段の通常動作を可能とする動作データを有する第１のＩＣカードと、前記取扱い手段が前記第１のＩＣカードを照合するための照合データを有する第２のＩＣカードを具備し、前記第２のＩＣカードから前記照合データが前記取扱い手段に登録され、登録された照合データを基に前記第１のＩＣカードの正当性が判断される。

【００２０】更に、本発明による第２のＩＣカード処理システムは、ＩＣカードに記録されたデータに基づいて動作するＩＣカード取扱い手段と、前記取扱い手段の通常動作を可能とする動作データ、及び前記取扱い手段との間で相互に認証するための第１の相互認証プログラムを有する第１のＩＣカードと、前記取扱い手段が前記第１のＩＣカードとの間で相互に認証するための第２相互認証プログラムを有する第２のＩＣカードを具備し、前記第２のＩＣカードから前記第２の相互認証プログラムが前記取扱い手段に登録され、登録された前記第２の相互認証プログラム及び前記第１のＩＣカードが有する前記第１の相互認証プログラムを基に、前記第１のＩＣカード及び前記取扱い手段は互いに認証を確認しあう。

6

【００２１】これにより上記（２．１）項で述べた秘密鍵等の漏洩に関する課題を解決することができる。又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードにより登録されたデータを、登録から一定時間後に自動的に消去する手段を更に有する。

【００２２】更に、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードにより登録されたたデータを、毎日一定時刻に自動的に消去する手段を有する。

【００２３】これにより上記（２．１）項で述べた秘密鍵等の漏洩に関する課題、及び（２．２）項で述べた盗難・不正使用に関する課題を解決することができる。又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記格納手段に格納された前記動作データを消去する手段を有する。

【００２４】又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が開かれたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有する。

【００２５】又、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体が破壊されたことを検出して前記格納手段に格納された前記動作データを消去する手段を有する。

【００２６】更に、本発明による第１又は第２のＩＣカード処理システムの前記取扱い手段は、前記第１のＩＣカードが有する前記動作データを格納する格納手段と、前記取扱い手段の筐体の蓋が破壊されたことを検出して前記筐体内部の時間・時刻データを無効化する手段を有する。

【００２７】これにより上記（２．１）項で述べた秘密鍵等の漏洩に関する課題、及び（２．３）項で述べた減算機の改造による不正使用に関する課題を解決することができる。

【００２８】又、本発明によるＩＣカード処理システムの前記取扱い手段は、プリペイドカード等として使用されるＩＣカードとの間で正当性確認情報を付加した電文を送受信することにより、前記ＩＣカードの正当性を確認する手段を有するこれにより上記（２．４）項で述べた不適合カードめ検査方法に関する課題、及び（２．５）項で述べた不正カード使用対策に関する課題を解決

することができる。

【００２９】又、本発明によるＩＣカード処理システムの前記取扱い手段は、複数の要因でＩＣカードの正当性を判断し、その判断結果により単なる不適合カードか偽造された不正カードかを判断する手段を有する。

【００３０】更に、本発明によるＩＣカード処理システムの前記取扱い手段は、不適合カードは排出し、不正カードは内部に取り込むかそのまま保持したまま他の機器へ発報する手段を有する。これにより上記（２．５）項で述べた不正カード使用対策に関する課題を解決することができる。

【００３１】

【発明の実施の形態】以下、この発明によるプリペイドカード用ＩＣカード処理装置の実施の形態を図面を参照して説明する。先ず始めに、機器の外観と機能構成ブロックの例をそれぞれ図１及び図２に示す。これは再度価値付け（増額）して再利用する運用形態のカード入金機４０である。この他に都度価値付けするカード販売機や、減算機能のみ持つ商品の販売機等があるが、本考案に関連する部分の最大構成を有するものとしてこれを示す。

【００３２】図１において、表示部４１はカード入金機４０を利用するための案内を表示する。カード差し込み口４３からカードは差し込まれ、金額選択ボタン４２により増額金額が入力され、金額投入・返却口４４から現金が投入又は返却される。テンキー４５は後述のキー登＊録カードのカードＩＤ等の値を管理者により入力するときに使用される。

【００３３】図２において、主制御部２は基本機能機能プログラムメモリ（ＲＯＭ）９に格納されたプログラムに従って、表示部４、入力部５、カード取扱い機構６、現金取扱い部７を制御する。主電源部３はＡＣ電源からＤＣ電源を発生し、主制御部２、ＲＯＭ９、表示部４、入力部５、カード取扱い機構６、現金取扱い部７に電源を供給する。バックアップ電源部８は主電源部３が動作していない時でも、常にメモリ１０ａ、１０ｂ、１０ｃに電源を供給する。

【００３４】本発明では従来の問題点を解決するための方策として次の５項目を説明する。

（３．１）登録カードによる主要データの登録

暗号・復号化プログラムや秘密鍵をプログラムメモリの内容を読み出すことにより入手することができないようにするため、機器への主要データ（主に機器動作用のデータ）のローディングは次のような項目を有する登録用ＩＣカードを使用する。

【００３５】（ａ）登録カード専用のフォーマット

（ｂ）登録カード専用のアクセス条件とキー値

（ｃ）登録カードごとに異なる所有者（使用者）暗証番号

このデータ登録カードの記録内容を表１に示す。

【００３６】

【表１】

データ・キー名称		内容の説明
カード内データアクセス用キー※	登録カードＩＤ	システムごとに異なる登録カードの身分証明番号 カード内で照合される読み出しできない照合用キー
	暗証番号	使用者が機器のテンキー等から暗証入力するキー カードごとに異なるいわゆる暗証番号
	相互認証用キー	本登録カードと機器の相互認証に使用されるキー このキー自体が照合されるのではない
機器へ登録するキーデータ	プリペイドカードＩＤ	実際の運用で使用されるカードのカードＩＤ
	相互認証用キー	プリペイドカード～機器の相互認証に使用されるキー
	正当性確認情報用キー	電文の正当性確認情報生成に使用されるキー
暗号ロジックまたはデータ		実際の運用で使用されるカードとのやりとりの中で必要とされる、機器側で実行される暗号処理のプログラム自体、又はそのプログラム動作に必要な主要データ

※照合用カード内データアクセス用キーの照合と相互認証処理が完了しない限り、他の読み出し・登録用のデータは読み出せない。

【００３７】このＩＣカードによるデータ登録は、機器をエンドユーザの元へ設置した後に実施することで、輸送中に盗難にあっても情報は漏洩しない。又、動作上の※重要データを有するカード、いわゆるキーカードの内容は機器のみが読出すことができるだけとし、それを使用するエンドユーザ自身に対しても知らせることなく運用

が可能である。尚、キーカードにより機器へ登録した各種の値を読出せない様にするための方法については後述する。

【００３８】この登録カードによる機器へのデータ登録操作と機器内処理の内容の例を図３に示す。先ず、操作者（管理者）により登録カードが機器に差し込まれる。機器側ではカードから得られる情報により、差し込まれたカードが登録カードかどうかを判定する。登録カード以外のカードが差し込まれた場合は適宜そのカードごとの処理へ移る。

【００３９】差し込まれたカードが登録カードであったならば、機器はそのカードで登録されるデータが既に登録済みであるかどうかを判定する。登録済みだった場合は差し込まれたカードのデータを新たに適用することで「書き換え」となるので、機器の設定として「書き換え」が許可されているかどうかを確認する。

【００４０】この機器の設定については製造時にシステムにあわせて固定値として設定しておいたり、製造後に登録カードによる本方法と同様の方法を含む種々の方法により設定することが考えられる。設定値としては、「書き換え不可」、「条件付き書き換え可能」、「無条件書き換え可能」等がある。「条件付き書き換え可能」の例として、金庫のダイヤルのように、カード挿入の回数及び時間間隔を設定することもできる。

【００４１】この設定で「書き換え」が許可された場合、及びデータが未登録の場合は次のステップへ移り、機器としてはカードの正当性を確認するべく相互認証をする。これがＯＫならば次は使用者の正当性確認のため、機器は操作表示部にメッセージを表示して操作者に対して暗証番号の入力を督促する。

【００４２】操作者によりその登録カードの暗証番号が入力されると機器はカードに対してその番号を照合し、ＯＫになってはじめて登録データの読出しに移る。この暗証照合がＮＧの場合、機器側の処理として登録データを読出しに行かないことは勿論だが、仮にこの状態でカードからデータを読出そうとしてもカードは暗証照合がＯＫとなっていないのでデータを出力しない。又、上記相互認証において、カード側が機器を正当な相手と判定していない場合は、例え暗証照合がＯＫとなってもカードはデータを出力しない。これらにより偽造された機器では登録データを読出すことはできない。

【００４３】このようにして読出された登録データは機器内のメモリに記憶されて、以降の機器動作に使用される。又、機器内のメモリに正常に記録されたことが確認された後、機器はカードを排出し操作者がこれを抜き取って保管する。

【００４４】次にこの様な機器の製造から運用に至るサイクルの例を、プリペイドシステム管理会社から機器供給を受けて運用するパチンコ店、ゲームセンタ等の遊技場での使用を例に図４に示す。

【００４５】先の登録操作と機器内処理の実施例では単純に一種類のカードでデータ登録する例を示したが、この実施例では実際のデータ（機器動作用データ）を登録するためのカードを「データ登録カード」として、この「データ登録カード」の使用を可能とするための各種のキーの値を設定する「キー登録カード」の２種類を使用している。

【００４６】「キー登録カード」で登録するキーとしては、上記登録操作と機器内処理の実施例で示した相互認証で使用するキーの他、登録カードであることを示すための照合用データであるカードＩＤ（キー）等がある。この２種類のカードの記録内容をそれぞれ表２及び表３に示す。

【００４７】

【表２】

データ・キー名称		内容の説明
カード内データアクセス用キー※	キー登録カードID	システムごとに異なるキー登録カードの身分証明番号 この値だけは本カードの使用前に機器に登録する
	暗証番号	使用者が機器のテンキー等から暗証入力するキー カードごとに異なるいわゆる暗証番号
	相互認証用キー	本登録カードと機器の相互認証に使用されるキー このキー自体が照合されるのではない
機器へ登録するキーデータ	データ登録カードID	データ登録カードのカードID
	相互認証用キー	データ登録カード～機器の相互認証に使用されるキー
	正当性確認情報用キー	データ登録カードと機器間の電文の正当性確認情報生成に使用されるキー

※照合用カード内データアクセス用キーの照合と相互認証処理が完了しない限り、
登録用キーデータは読み出せない。

【0048】　　＊　＊【表3】

データ・キー名称		内容の説明
カード内データアクセス用キー※	データ登録カードID	システムごと異なるデータ登録カードの身分証明番号 キー登録カードにより登録される
	暗証番号	使用者が機器のテンキー等から暗証入力するキー カードごとに異なるいわゆる暗証番号
	相互認証用キー	本登録カードと機器の相互認証に使用されるキー このキー自体が照合されるのではない
正当性確認情報用キー		
機器へ登録するキーデータ	プリペイドカードID	実際の運用で使用されるカードのカードID
	相互認証用キー	プリペイドカード～機器の相互認証に使用されるキー
	正当性確認情報用キー	電文の正当性確認情報生成に使用されるキー
暗号ロジックまたはデータ		実際の運用で使用されるカードとのやりとりの中で必要とされる、機器側で実行される暗号処理のプログラム自体、又はそのプログラム動作に必要な主要データ

※照合用カード内データアクセス用キーの照合と相互認証処理が完了しない限り、
登録用データは読み出せない。

【0049】キー登録カードは次のような運用が考えられる。
（a）例えば一店舗を一つのシステムと見なし、1システム（各店）ごとに1枚作成し管理会社が保管・使用する。
【0050】（b）基本的に機器の設置時、その店のシステムの初期設定として管理会社がこのカードを使用して、そのシステム（店舗）で使用するデータ登録カードのアクセスキーを機器へ登録する際に使用する。
【0051】（c）事故等でその店舗の機器のキーデー※50タが消えてしまった場合や、データ登録カードのアクセスキーの値にに変更が生じた場合には、管理会社が出向いてそのキーを機器へ再登録する。
【0052】（d）キー登録カード自体の暗証番号の他、データ登録カード使用に先だって暗証番号を入力しないとデータ登録カードが使用できないようにすることもできる。
【0053】又、データ登録カードは次のような運用が考えられる。
（a）例えば一店舗を一つのシステムと見なし、1シス

テム（各店）．ごとに1枚～数枚作成し、店舗のシステム管理者が保管・使用する。

【００５４】（ｂ）基本的に毎朝、昨夜（昨営業日）の深夜０時で自動消去されてしまった機器の動作用データを再登録する際に使用する。これにより機器は当日の深夜０時まで使用可能となる。

【００５５】（ｃ）データ登録カード自体のＩＤ番号の他、データ登録カード使用に先だって暗証番号を入力しないと登録カードが使用できないようにすることもできる。図４に示すこれらのカードを使った機器の使用例の流れは次のようになる。

【００５６】機器はメーカにて、カードのハンドリング、表示、通信制御と、カードを使った各種処理の基本部分を搭載した機器として製造される。機器はメーカから管理会社へ納入されるか、管理会社からの指示により設置場所へ直接納入され、管理会社の担当者立ち会いのもとユーザの遊技場（店舗）に設置される。このとき、管理会社の担当者がキー登録カードを使用して、データ登録カードのアクセスキーデータを機器へ登録する。このキー登録カードを使用するには、機器側にキー登録カードのカードＩＤが登録されている必要があり、これについては固定値として製造時に機器に登録してしまうか、機器のテンキーから管理会社の担当者が入力する等が考えられる。又、このとき店舗ごとに記録データの異なるデータ登録カードをユーザ側へ引き渡し、機器の運用管理は遊技場に任される。

【００５７】店側ではデータ登録カードを使って、このカードを管理する責任者（システム管理者）により、機器動作用のデータを機器へ登録する。このデータ登録が完了した後、機器は実際に使用可能となる。

【００５８】ここで、本実施例では３．２項として以下に示される「キーカードによる使用時間延長」の機能も盛り込んでいる。即ち、店のシステム管理者がデータ登録カードで登録したデータが機器内部の時計により、登録後の一定時間か、時刻としての一定時刻に自動消去するようにしておき、データ登録カードを使用して再度登録しなくては使用不可能となるように設定できる。４図では後者の一定時刻として深夜０時でデータが消去され、翌朝又は翌営業日開店前に再登録するものとしている。このような運用により、店舗が無人となる深夜や休日まで使用できない状態となり、盗難されてもデータ登録カードがなければ不正使用されることはありえない

（３．２）データ登録カードによる使用時間延長（カード販売機について）

価値付けされていないカードを投入金額に応じて都度価値付けして販売するものや、カードを再利用する運用形態で入金機として機能する機器において、価値付けされていないカードが手に入っても、その販売機を使用して正当な代価を支払うことなく自由な金額でカードに価値付けできないようにするために、一定時間に一回、使用許可キーカードを差し込まないと自動的に使用不能とする。

【００５９】この方式の実施例は、データ登録カードを使用許可を与えるキーカードとして利用し、玉貸金額書込機内のカレンダの日付が変わると書込機内の各種キーの値が自動消去される例を「３．１登録カードによる主要データの登録」の運用例として記載している。

【００６０】（３．３）　開蓋・破壊時データ消去

以下の手法により、機器のケースを開く等すると動作に必要な機器内の主要データが消云される。

【００６１】動作に必要なデータの主要部分はＲＯＭには載せずにハードウェアの完成後外部からＲＡＭ等の揮発性のメモリ部分へローディングするものとし、ケースを開いたり破壊したりするとこのメモリの内容の保持動作（回路）が中断（切断）しメモリ内のデータを消すことで、それ以降は動作不能とする。

【００６２】この方式の実施例は運用例として「データ登録カード」とそのカードのアクセス用キーを登録する「キー登録カード」により、機器へ動作に必要なデータを登録する部分を「３．１　登録カードによる主要データの登録」の運用例の中に記載している。

【００６３】以下に構造案の実施例を示す。

（ａ）蓋開センサ／スイッチ方式

この筐体構造の断面図を図５に示す。筐体の蓋２０が開かれると解放する光センサスイッチＳＷ１又は機械スイッチＳＷ２、ＳＷ３を介して、バックアップ電池８による電源が供給されることで静的（Ｓｔａｔｉｃ）に内容が保持されている揮発性メモリ（ＳＲＡＭ等）１０にデータを記録することで、蓋２０が解放されスイッチが解放された瞬間にバックアップ電源が断たれメモリ内容は揮発する。

【００６４】（ｂ）入射光センサ方式

この筐体構造の断面図を図６に示す。光が入射すると回路を解放する光センサスイッチＳＷ４、ＳＷ５を介してバックアップ電池８による電源が供給されることで静的に内容が保持されている揮発性メモリ１０にデータを記録することで、蓋２０が解放され光センサスイッチに光が入射した瞬間にバックアップ電源が断たれメモリ内容は揮発する。

【００６５】（ｃ）筐体回路パターン方式

この筐体構造の断面図を図７に示す。図７（ｂ）に示すように、筐体の素材内に巡らされた回路網を通してバックアップ電池８による電源が供給されることで静的に内容が保持されている揮発性メモリ１０にデータを記録することで、筐体の一部が破壊され回路網が途絶した瞬間にバックアップ電源が断たれメモリ内容は揮発する。筐体全体に回路網を通す構造が理想だが、ここでは蓋部材に回路網を通し基板上のコネクタで接続する方式例の筐体構造を示す。

【００６６】以上の実施例は全て、筐体を開こうとした

際に揮発性メモリ１０のバックアップ電源を断つ方式だが、これらの蓋・筐体を開いたことを検出する手法を利用し、次のようにメモリのデータを消すことも可能である。尚、これらを複合して使用することも十分考えられる。

【００６７】（ｄ）DRAM保持動作中断方式

この方式の動作の流れを第８図に示す。データを動的（Ｄｙｎａｍｉｃ）にメモリ保持動作をする形式のメモリ（DRAM等）に記録し、蓋・筐体が開かれたことをきっかけにこのメモリ保持動作を中断する。具体的にはDRAM１０のメモリ保持動作（リフレッシュ）に不可欠なクロック信号の供給を主制御部２から制御できる回路構成としておき、蓋・筐体が開かれたことをスイッチ、センサ等で検出したらこのクロック信号を止める割り込み処理を起動することで実現できる。

【００６８】（ｅ）消去プログラム起動方式

この方式の動作の流れを図８に示す。上記の様なバックアップ電源に関する処置をしていない、常にバックアップされ続けるメモリにデータを記録し、蓋・筐体が開かれたことをきっかけにこのデータを消去するプログラムを強制起動する。具体的には、消去すべきデータが格納されているメモリに対してスペースやＮＵＬＬ等意味のないダミーデータを書き込む割り込み処理を用意しておき、蓋・筐体が開かれたことをスイッチ、センサ等で検出したらこの割り込み処理を起動することで実現できる。

【００６９】以上は登録データを消去することを主旨に説明したが、この手法は（３．２）に示した「使用時間延長」の処理で使用する機器内の時計が進まないように改造することの防止にも応用できる。即ち機器内の時計が進まないように改造することでキーカードによる時間延長を不要とし、永続的に使用できるようにすることができるため、蓋が開かれたり筐体が破壊された場合、時間・時刻データを無効化することで不正使用を防ぐことになる。

【００７０】（３．４）電文正当性確認

秘密鍵をカードと機器で持ち合い、相互に共有する何らかのデータを秘密鍵を用いて暗号化し、暗号化されたデータを正当性確認情報として電文の一部として含め、その電文が正当な相手から送られてきたものであることを正当性確認情報の内容により、カードと機器双方が確認する。

【００７１】機器から送られてきた電文のカード側での確認は、主として偽造された機器による正当なカードに対する金額の書込（増額）を防止し、カードから送られてきた電文の機器側での確認は、主として偽造されたカードによる正当な機器での買い物（購入）を防止する。又、機器側がカードを不正と判定した場合、そのままカードを保持し警報を発したり、機器内部に回収することも可能である。

【００７２】以下にカードと機器双方における正当性確認手順の例を示す。又、これらを複合して各々で電文の正当性を確認するやりとりの例を図１０に示す。図１０はカードの残高を減額し商品を販売するような運用形態を示す。このような処理の使用例としては、カード側での機器からのコマンド電文の正当性確認は偽造された入金機による正規カードへの入金を防止し、機器側でのカードからの実行結果通知電文の正当性確認は偽造カードによる商品等購入を防止する効果が狙いとなる。従って図１０のように相互に正当性確認を実行することは少ないと考えられる。即ち、偽造カードに正規の入金機で現金を支払って入金することも、商品販売に使用する減額機器を偽造することも、いずれも（不正な）利益は生み出さないためである。しかし、使用者が偽造カードと知らない場合等に後述の３．５に示す様な不正カードを回収し、出所を探るためには有効でる。尚、金額書き換えコマンドの使用に至る前に、カードと機器相互に正当な相手であることを確認するための「相互認証」を実行する後述の３．５に示す様な運用形態も考えられ、本実施例と併用することも可能である。

【００７３】次に図１０の動作によるカード側での正当性確認を説明する。以下の手順で機器からの金額書き換えコマンド自体の正当性を確認し、正当と判定されたときのみカードは金額書き換えを実行する。

【００７４】（ｓｔＡ）　金額書き換えに先立ち機器がカードに対して乱数出力を要求しカードがこれに応える。

（ｓｔＢ）　機器側では取得した乱数を基にこれから書き込もうとする書込日、書き込み金額を秘密鍵で暗号化する（この暗号化されたデータが正当性確認情報である）。

【００７５】（ｓｔＣ）　機器からカードへステップｓｔＢで生成したデータを金額書き換えコマンド電文の一部として送信する（書込日、更新金額も電文に含めて送る）。

【００７６】（ｓｔＤ）　金額書き換えコマンド電文を受けたカードは先に送出した乱数を基に、内部で同様の暗号化により正当性確認情報を生成し、電文内の同データと比較することで機器からの電文の正当性を確認し、照合ＯＫのときにのみカードは金額書き換えを実行する。

【００７７】（ｓｔＥ）　照合がＯＫでなかった場合、カードは機器に対して処理実行否定通知を送る。この例は減額機器の場合を示しているが、カード側での機器からの電文の正当性確認情報の照合（ｓｔＤ）は、偽造された入金機（増額機器）による正規カードへの入金を防止することができる。

【００７８】次に図１０の動作による機器側での正当性確認を説明する。上記カード側での正当性確認のステップｓｔＤにおいて、カード側で電文を正当と判定し金額

書き換えが実行されると、処理結果の如何に関わらずカードは機器に対して実行結果通知レスポンス電文を返す。このとき次の手順によりカードからの結果通知電文自体が正当なものであるかどうかを確認し、正当と判定されその内容が金額書き換え処理が正常終了を示すときのみ機器はカードに対する処理を実行する。

【００７９】（ｓｔＦ）　金額書き換えを実行したカードは、金額書き換えコマンド電文の一部として機器から受け取つた現在時刻、引き去り金額等を、暗号化用秘密鍵を用いてカード内で暗号化する（この暗号化されたデータが正当性確認情報）。

【００８０】（ｓｔＧ）　カードから機器へステップｓｔＦで生成したデータを、書き込みコマンド電文の実行結果通知（応答）電文の一部として送信する。

（ｓｔＨ）　実行結果通知（応答）電文を受けた機器は、内部で同様に正当性確認情報を生成する。

【００８１】（ｓｔＩ）　生成した正当性確認情報と電文内同データと比較することで機器かの電文の正当性を確認し、照合ＯＫのときにのみ機器はそのカードを使用して所望される動作の最終段階（例えばプリペイド自販機による商品購入時の商品の送出）を実行する。

【００８２】（３．５）　不正カード使用発報

「相互認証」や「実行結果（応答）電文正当性確認」により、使用されたカードが不正カードであると判定された際、機器はそのカードを内部に保持したまま機器の管理者側（ホスト）へ通知（即時発報）する。これにより使用された不正カードを回収したり、使用者を特定することができる。具体的動作の流れを図１１に示す。又、図１２に複数の機器３０とそれにオンライン接続されたホスト３１構成されるシステムを示す。

【００８３】機器はカードが差し込まれるとカードを活性化する。活性化時に機器が受け取るカードの初期応答（アンサトゥリセット）については、別種の用途のカードでは機器側で所望の値ではない場合も多く、単なる不適合カードとして排出すればよい。この初期応答が所望の値だった際、機器はカードＩＤの照合に移る。カードＩＤについては用途・システムにより様々な値とすることが当然であり、照合ＮＧの場合やはり単なる不適合カードとして排出すればよい。

【００８４】カードＩＤの照合がＯＫだった場合、引き続き相互認証の処理に移る。相互認証についてはカードＩＤが一致した場合、基本的に（カードやデータが壊れていない限り）不成立となることはなく、不成立の場合それはほぼ不正カードであると判断して間違いない。この不成立の内容には、相互認証機能がない、相互認証に使用される乱数生成ロジックが異なる、同一のロジックでも使用するキー値が異なる、等が考えられる。このとき機器はそのカードを内部に保持したまま使用者には判らないように不正カードが使用されたことをオンラインでホストへ即時に発報する。

【００８５】相互認証が正常に終了した場合、引き続き金額書き換え処理に移る。この金額書き換えでは、電文の正当性確認を行なうが、相互認証までもが正常に終了した場合、カードＩＤが一致しただけより更に正当性確認情報が不整合となることはなく、不整合の場合それはほぼ不正カードであると判断して間違いない。このとき機器はそのカードを内部に保持したまま使用者には判らないように不正カードが使用されたことをオンラインでホストへ即時に発報する。尚、この不整合の原因には、上記相互認証が不成立となる要因と同様、不正カードに、機能がない、ロジックが異なる、キー値が異なる等がある。

【００８６】３．１に示したプリペイドシステム管理会社から機器供給を受けて運用するパチンコ店、ゲームセンタ等の遊技場の例においては、発報を受けたホストは該当する機器を特定する情報を表示するので、係員は発報した機器へ出向きそのカードを回収するとともに、使用者に事情を聞くといった運用が可能である。又、不正カードを機器の内部に回収してしまうことは３．１の例に限らず適用可能である。

【００８７】

【発明の効果】本発明により、プリペイド用ＩＣカードと処理装置を偽造・変造されにくくできる。即ち、プリペイド用ＩＣカード等の高セキュリティ化されたカードのセキュリティレベルを機器やデータ管理面で低下することがないだけでなく、システム全体をより高セキュリティ化することができる。

【図面の簡単な説明】

【図１】ＩＣカード入金機の外観を示す。

【図２】ＩＣカード入金機の機能構成を示すブロック図。

【図３】本発明の登録カードによる機器へのデータ登録操作と機器内処理を示すフローチャート。

【図４】プリペイド用ＩＣカード取扱い機器の製造から運用に至るサイクルの例を示すフローチャート。

【図５】蓋開センサ／スイッチ方式の筐体断面図。

【図６】入射光センサ方式の筐体断面図。

【図７】筐体回路パターン方式の筐体断面図。

【図８】ＤＲＡＭ保持動作中断方式の動作を示すフローチャート。

【図９】消去プログラム機動方式の動作を示すフローチャート。

【図１０】ＩＣカードと機器双方で電文の正当性を確認するやりとりの例を示す図。

【図１１】不正カード使用時の発報処理動作を示すフローチャート。

【図１２】機器とホストをオンライン接続した構成を示す図。

【符号の説明】

２…主制御部

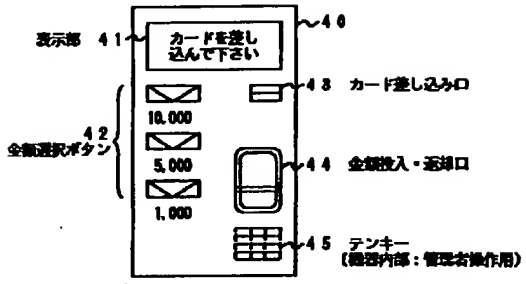
19

3…主電源部
4…表示部
5…入力部
6…カード取扱い機構
7…現金取扱い部
8…バックアップ電源部

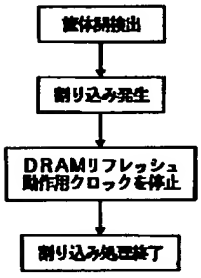
20

9…プログラムメモリ
10a…ワーキングメモリ
10b…暗号機能プログラムメモリ
10c…キーデータメモリ
40…カード入金機

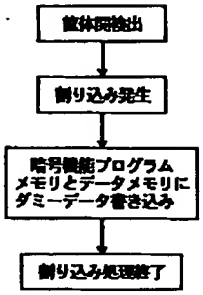
【図1】



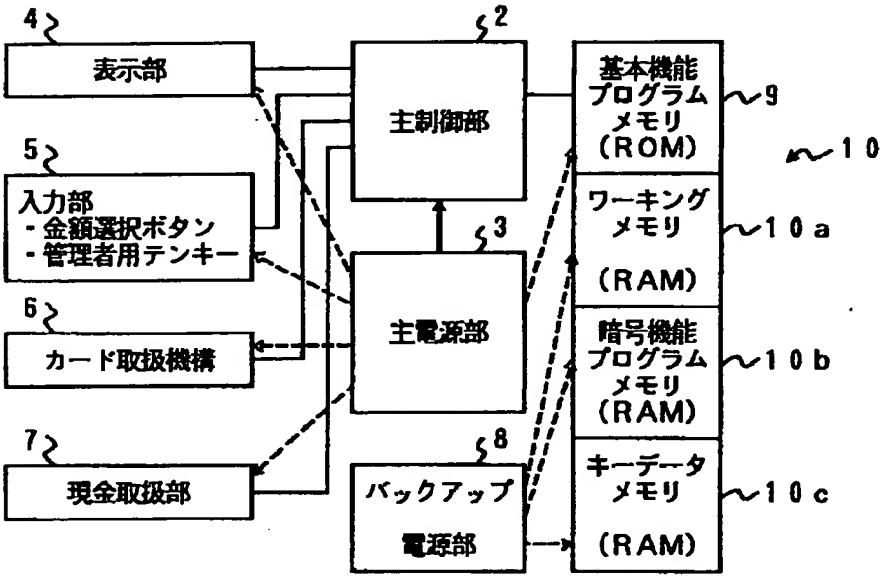
【図8】



【図9】

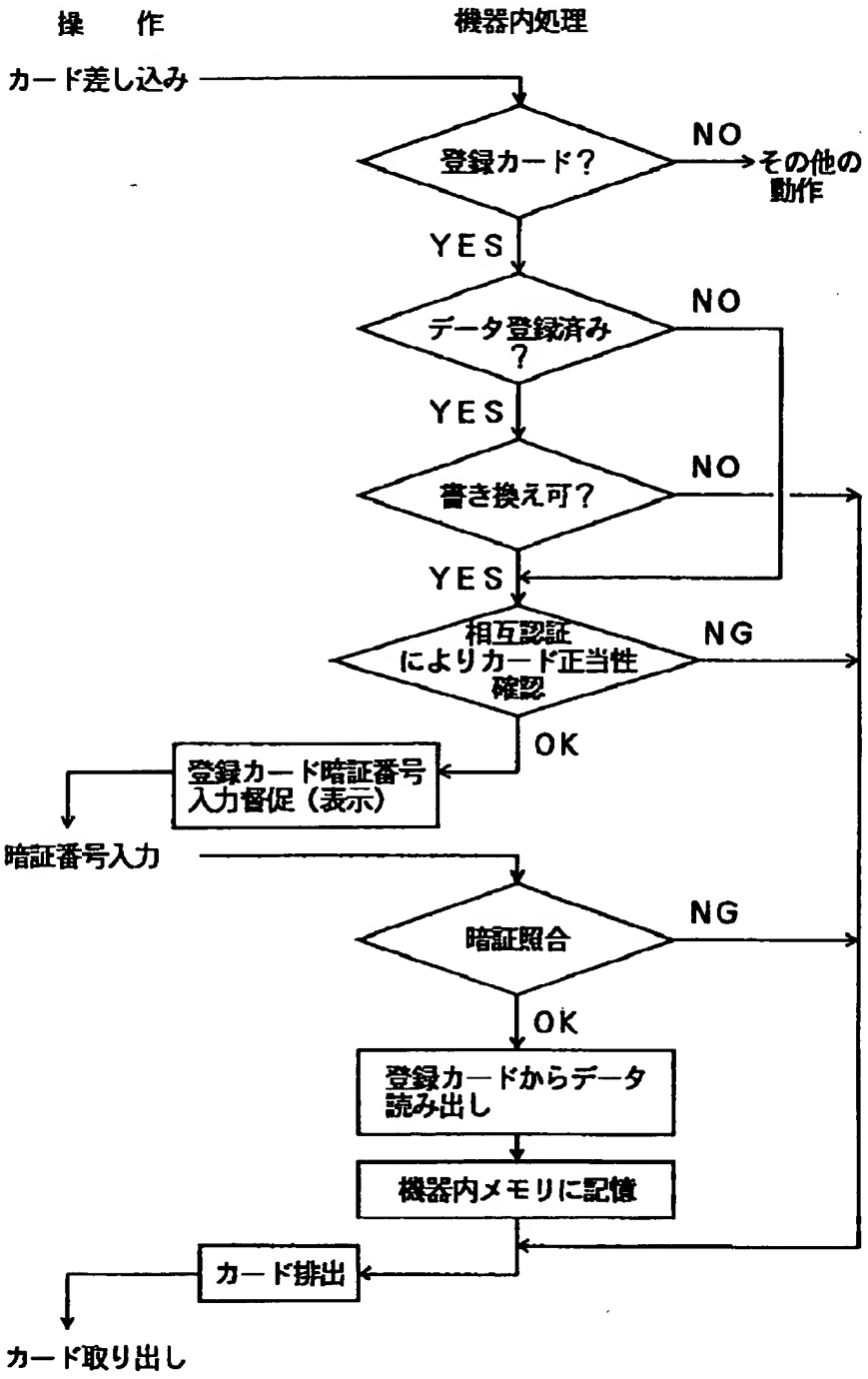


【図2】

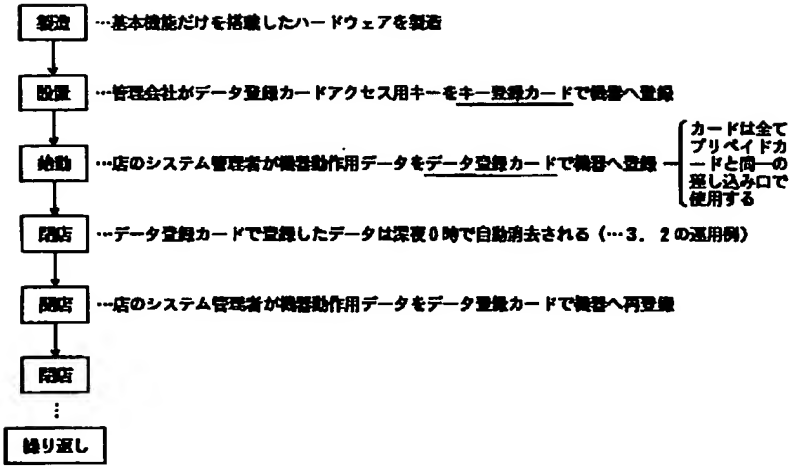


[——— ：制御　　------ ：電源]

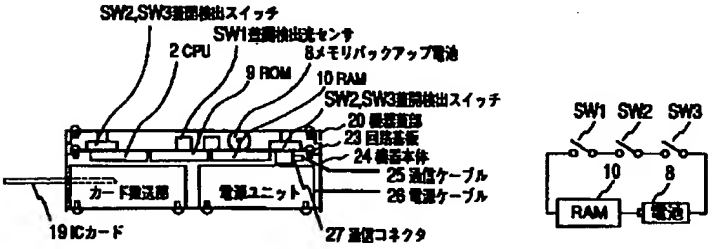
【図3】


操　作
機器内処理
カード差し込み
登録カード？
NO
その他の動作
YES
データ登録済み？
NO
YES
書き換え可？
NO
YES
相互認証によりカード正当性確認
NG
OK
登録カード暗証番号入力督促（表示）
暗証番号入力
暗証照合
NG
OK
登録カードからデータ読み出し
機器内メモリに記憶
カード排出
カード取り出し

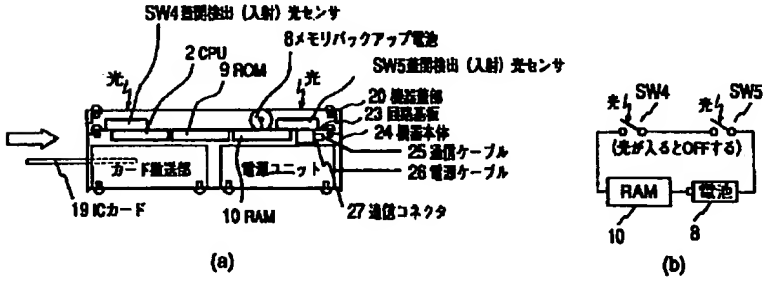
【図4】


製造
…基本機能だけを搭載したハードウェアを製造
設置
…管理会社がデータ登録カードアクセス用キーをキー登録カードで機器へ登録
始動
…店のシステム管理者が機器動作用データをデータ登録カードで機器へ登録
カードは全てプリペイドカードと同一の差し込み口で使用する
閉店
…データ登録カードで登録したデータは深夜0時で自動消去される（…3．2の運用例）
開店
…店のシステム管理者が機器動作用データをデータ登録カードで機器へ再登録
閉店
繰り返し

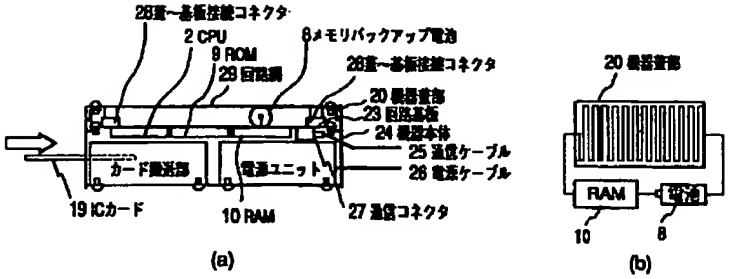
【図5】


SW2,SW3遮断検出スイッチ
SW1遮断検出光センサ
2 CPU
8メモリバックアップ電池
9 ROM
10 RAM
SW2,SW3遮断検出スイッチ
20 機器筐体
23 回路基板
24 機器本体
25 通信ケーブル
26 電源ケーブル
カード読込部
電源ユニット
19 ICカード
27 通信コネクタ
(a)
SW1 SW2 SW3
10
8
RAM
電池
(b)

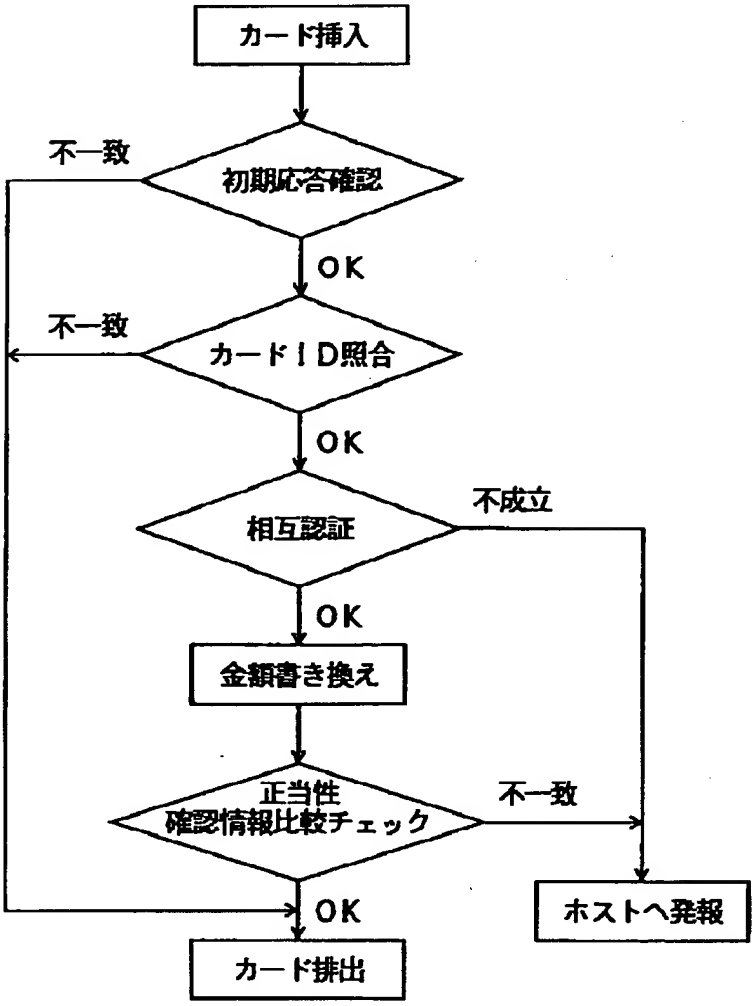
【図6】


SW4遮断検出（入射）光センサ
8メモリバックアップ電池
2 CPU
9 ROM
SW5遮断検出（入射）光センサ
光
光
20 機器筐体
23 回路基板
24 機器本体
25 通信ケーブル
26 電源ケーブル
カード読込部
電源ユニット
19 ICカード
10 RAM
27 通信コネクタ
(a)
光
SW4
光
SW5
(光が入るとOFFする)
RAM
電池
10
8
(b)

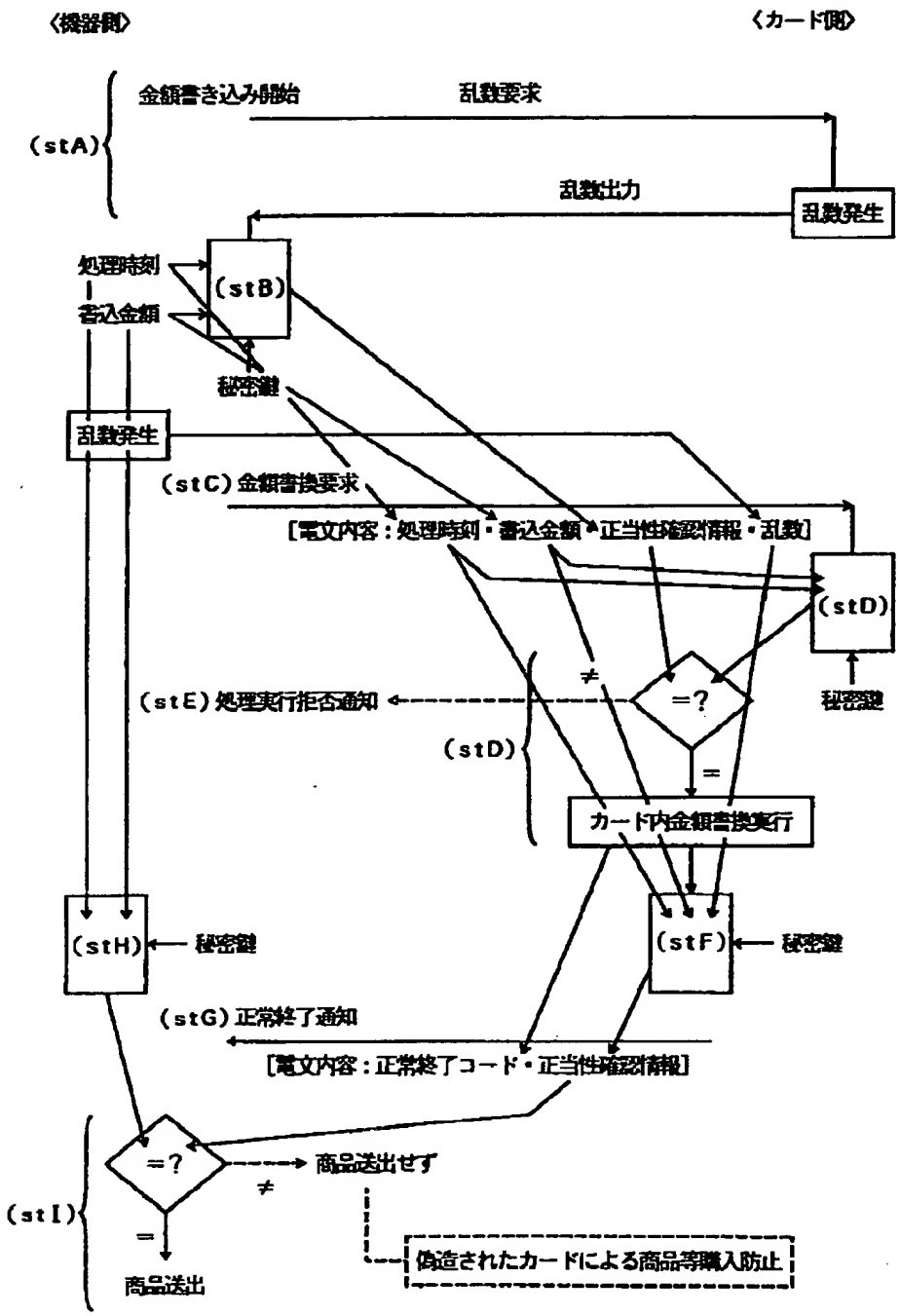
【図7】


2 CPU
9 ROM
8メモリバックアップ電池
20 機器書換
23 回路基板
24 機器本体
25 通信ケーブル
26 電源ケーブル
カード挿入部
電源ユニット
19 ICカード
10 RAM
27 通信コネクタ
(a)
20 機器書換
RAM
電池
10
8
(b)

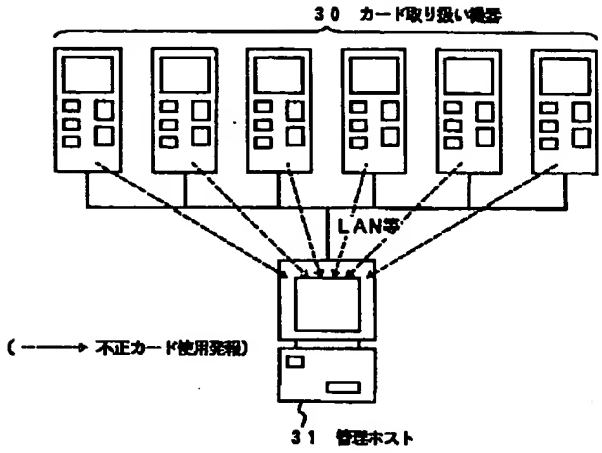
【図11】


カード挿入
初期応答確認
不一致
OK
カードID照合
不一致
OK
相互認証
不成立
OK
金額書き換え
正当性
確認情報比較チェック
不一致
OK
ホストへ発報
カード排出

【図10】


〈機器側〉
〈カード側〉
(stA)
金額書き込み開始
乱数要求
乱数出力
乱数発生
処理時刻
書込金額
(stB)
秘密鍵
乱数発生
(stC) 金額書換要求
[電文内容：処理時刻・書込金額・正当性確認情報・乱数]
(stD)
秘密鍵
≠
=?
(stE) 処理実行拒否通知
(stD)
=
カード内金額書換実行
(stH)
秘密鍵
(stF)
秘密鍵
(stG) 正常終了通知
[電文内容：正常終了コード・正当性確認情報]
=?
商品送出せず
≠
(stI)
=
商品送出
偽造されたカードによる商品等購入防止

【図12】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
G07F 7/12			G07F 7/08	S	
				C	

2416065 Supplier Number: 02416065 (THIS IS THE FULLTEXT)

Smart Cards: Java Gets Pats on Back From Card Businesses In Belgium and France

(Proton World International, Bull Group to boosting the Java language of Sun Microsystems regarding smart cards)

American Banker, v 164, n 61, p 16
March 31, 1999
DOCUMENT TYPE: Newspaper ISSN: 0002-7561 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1111

ABSTRACT:
Proton World International of Belgium, a major smart card organization, announced it would distribute a version of its electronic purse based on the Java Card API, or application programming interface.

Proton started as part of the Banksys payment system consortium in Belgium. It has 30+ million electronic purse cards operating on its system in 15 countries. The company said its Java e-purse would be included in the next generation of multiple-application cards.
A second firm, Bull Group of France, established a joint venture with a national research institute to work on developing open-standards-based microprocessor cards, with Java key among those standards.

Known as Trusted Logic, the new venture is to research, develop, and sell sophisticated levels of security, prove their workability in electronic banking and other fields, and perhaps profit further by licensing intellectual property.

TEXT:
By JEFFREY KUTLER

Two major smart card organizations in Europe have given Sun Microsystems Inc.'s Java language a boost.

Proton World International of Belgium said it would distribute a version of its electronic purse based on the Java Card API, or application programming interface. The e-purse applet will be easily linked to other services on a smart card, such as ticketing and loyalty, Proton said.

In France, Bull Group formed a joint venture with a national research institute to develop open-standards-based microprocessor cards, with Java key among those standards.

The new venture, Trusted Logic, is to research, develop, and sell sophisticated levels of security, prove their workability in electronic banking and other fields, and perhaps profit further by licensing intellectual property.

These moves, announced last week, may say more about the smart card industry's desire for technical common denominators than about Java specifically. The Java Card specification is vying with Multos, which is associated with the Mondex smart card system, and with Microsoft Corp.'s Smart Cards for Windows. Each lays claim to being an open framework that invites innovation.

But with the Microsoft entry in the market for less than half a year, and with Multos still fending off criticism that it is more proprietary than open, Java seems to be taking advantage of its relative maturity. The language itself is about four years old and well suited to Internet transactions, including the remote loading of applets-small software applications-or other data onto smart cards.

Proton officials have long expressed support for Java, a position reinforced last year when Visa International, a Java partisan, took an equity interest in the Brussels-based smart card company.

Dominique Bolignano, chairman of Trusted Logic, said advances in theoretical technology and programming languages are accelerating just as "demand is developing significantly" for smart card systems in mobile phones, payment terminals, and elsewhere. "The catalyst for this change will be Java," he said.

The Java Card API dates to 1996. Its 2.0 version followed in October 1997, and 2.1 enhancements came out in October 1998.

Visa embraced Java for its Visa Open Platform program. Proton World-co-owned by American Express Co., Banksys of Belgium, ERG Ltd. of Australia, and Interpay of the Netherlands-bills itself as a "strategic business partner" of the Java Card Forum, which has a strong hand in setting the technical specifications. Forum members include major chip card manufacturers and International Business Machines Corp., Citibank, and National Westminster Bank of London. Natwest invented Mondex and later sold most of its shares to MasterCard International and about two dozen financial institutions around the world.
Proton, which began as part of the Banksys payment system consortium in Belgium and has more than 30 million electronic purse cards operating on its system in 15 countries, said its Java e-purse would be incorporated into the next generation of multiple-application cards.

The stored-value program will "remain at the cutting edge of smart card technology through this important new development with Sun," said Yves Moulart, Proton World's executive vice president of research and development.

Patrice Peyret, director of Sun Microsystems' consumer and embedded division in California, said Proton on the Java Card API "enriches the selection of financial services available" for Java smart cards.

"Proton World is a leader in the deployment of secure smart card technology worldwide," Mr. Peyret said. "This applet demonstrates Sun's continuing efforts to work with strategic associates to make Java Card the premier solution for multi-application smart cards."

Trusted Logic-the result of collaboration between Bull Smart Cards and Terminals and INRIA, the French National Institute for Research in Computer Science and Control-will be applying a mathematical technique, formal proof, to bolster smart cards' ability to withstand security threats.

Formal proof is a requirement of Common Criteria, a set of internationally recognized security standards on which microprocessor and data security vendors, among others, are seeking to be rated.

"With the arrival of open platforms such as Java, guaranteeing and proving security has become essential," said Christian Goire, a Bull executive, who also serves as chairman of Java Card Forum. "I am delighted with the

creation of Trusted Logic, since it corresponds to the needs expressed by the forum's strategic partners in the banking and telecom sectors."

Bernard Larrouturou, chairman of INRIA, said, "Fifteen years of research will now be applied to the fast-expanding market of smart cards, a market where European manufacturers, in particular Bull, are the world leaders." He said Bull and INRIA "have made great headway in terms of research and its subsequent marketability, and, thanks to Dominique Bolignano, (this) led to the creation of a high-tech company."

David Levy, managing director of Bull Smart Cards and Terminals, said a desire to expand in the field of open systems such as Java motivated Bull's participation in Trusted Logic. The efforts with formal proof "will play an essential role in demonstrating the security of future smart card applications," he said. "Bull thus strengthens its position as No. 1 in the field of security." That claim is likely to be disputed, but it indicates that security is becoming a competitive battleground.

IBM, which does joint Java Card development with Gemplus of France, made a recent deal with Philips Semiconductors to pursue chips that can pass muster with Common Criteria or with the related ITSEC methodology-Information Technology Security Evaluation Criteria.

Mr. Peyret said "Sun is very enthusiastic about the arrival of Trusted Logic in the microprocessor card software industry. It goes to show that open systems such as Java favor new actors with new services."

He praised "Trusted Logic's key actors" for past contributions to the development of Java Card API and said "their know-how in this domain should give them an excellent start."

u

Bull Smart Cards and Terminals said it has demonstrated a system for loading value onto smart card chips via mobile telephone.
The system is based on Sun Microsystems Inc.'s Java technology and can be used in phones with two card slots conforming to the GSM, or Global System for Mobile communications, standard.

Bull's major chip card rivals, including Gemplus and Schlumberger, have also been developing remote commerce applications for GSM phones. The market for chip-based SIM cards-subscriber identity modules required to authenticate users of those phones-is one of the most active in the smart card industry.

The demonstration this month involved a Bull Rock'n Tree SIM card in one phone slot, and a Proton electronic purse card in the other. With a call to a bank's e-purse server, the phone plays the role of a reloading terminal.

Bull said that through its SIM Rock'n Lab, such applications can be "developed in record time, even by users with no knowledge of the Java language."

COMPANY NAMES: GROUPE BULL; PROTON WORLD INTERNATIONAL SA
INDUSTRY NAMES: Payment cards
PRODUCT NAMES: Prepayment smart cards (367933)
CONCEPT TERMS: All market information; All product and service information

; Product development; Users
GEOGRAPHIC NAMES: Belgium (BEL); European Union (EUCX); France (FRA);
Western Europe (WEEX)
?
?

Record: 1

Title: Of Elvis and smart card sightings.
Authors: Do, Alyxia
Source: Automatic I.D. News; May97, Vol. 13 Issue 6, pS.20, 2p, 1c
Document Type: Article
Subject Terms: *SMART cards
Abstract: Discusses smart cards technology. Key characteristics of smart cards compared to other identification technologies; Cost of smart cards; Smart cards' high degree of application-technology fitted for applications which either need security or must handle an immense amount of data.
Full Text Word Count: 1077
ISSN: 0890-9768
Accession Number: 9709031038
Database: Business Source Corporate

Section: FEATURE

OF ELVIS AND SMART CARD SIGHTINGS

Soon, only one will be an American myth

These days in the United States, smart cards are a lot like spotting Elvis. Everyone in America keeps talking about his being in supermarkets, subways and banks--but have you really seen the King of Rock-n-Roll lately?

Yeah, me neither.

Everywhere from Scientific American to USA Today, articles on smart cards are proclaiming them to be the latest and greatest. The marketing hype is there, but where are the cards? Indeed, market development in the United States will take at least two more years. Industry participants, however, are gearing up for what may be in several years a billion-dollar American market. Add into that equation Latin America and the Asia-Pacific regions, where smart card markets are picking up speed, and we're talking about potential market revenues of several billion dollars. Smart cards are a substitute for some traditional automatic identification technologies in several applications--but where and how and why?

Stacking up smart cards against other technologies

Smart cards have three key characteristics compared to other technologies:

Increased data storage and computational capacity.

Increased security that can handle open systems.

Offline transaction-handling capability

In all three areas, neither magnetic stripe nor bar code technologies are comparable to smart cards. While magnetic stripe and bar code systems may have password protection procedures, the data carrier itself does not have built-in security. When France Telecom moved from magnetic stripe cards to smart cards for its prepaid phone card application, fraud costs were cut by 50%.

RF/ID trends in increased data storage and security capacities make them more competitive to smart cards than magnetic stripes or bar codes. Contactless smart cards, however, possess a significantly higher data transfer rate than RF/ID tags: 100 Kbits/second versus 4 Kbits/second, respectively RF/ID tags, however, do have the advantage of a longer read/write distance (up to 3 feet versus the 4 inches of a contactless smart card). Still, a contactless smart card can be an ideal choice

for RF/ID target markets such as transportation and security access.

Moreover, a unique characteristic of smart cards which propels their growth in developing countries is their ability to handle of Dine transactions. Online systems such as ATMs or EFTPOS demand access to a central host or database to perform transactions. Hence, for countries such as China, which has three main telephone lines per 100 inhabitants, or Brazil, which has seven main lines per 100 inhabitants, ATMs and prepaid public phone cards are not practical Smart cards provided these countries an opportunity to acquire traditional online systems without the infrastructure investment cost. For this reason, smart cards are taking off in Latin America and the Asia-Pacific region.

The price is right--per byte

The increased performance of smart cards, however, also brings a higher price tag--or does it? On the surface, a smart card costs quite a bit more per unit--more than twice its nearest competitor, the RF/ID tag. Yet, m terms of a price/memory performance ratio, smart cards remain highly competitive. Indeed, in regards to RF/ID tags, smart cards cost approximately 81% less per data storage byte.

Moreover, in the next three to five years, smart cards will be an even greater bargain as average selling prices drop further. Since 1993, the average selling price of a smart card has dropped approximately 15% annually, and industry participants do not expect prices to bottom out soon. None of the price levels of the other technologies is likely to decline as dramatically; in fact, magnetic stripe and bar code price levels are likely to remain flat. Consequently, with increasing chip capabilities and decreasing prices, smart cards will offer increasingly better performance at lower prices.

How smart cards make the fit

Still, the basic fact is that smart cards in the future will still cost mote than magnetic stripe or bar code technologies. Indeed, in certain applications smart cards will not be likely substitutes for other technologies because the degree of the application-technology fit is too low. Inventory tracking, for example, may not require a smart card's increased data storage or security features.

Smart cards, however, have a very high degree of application-technology fit for applications which either need a high level of security or must handle an immense amount of data. The GSM (global system for mobile communications) application is a good example. A type of wireless communication platform, GSM competes actively against cellular networks as a service choice. Analysts estimate that in the United States, cellular fraud costs service providers up to $1.5 million a day. On the other hand, the GSM platform incurs minimal fraud losses due to a subscriber identity module (SIM), which is provided by a smart card as a means of user authentication.

In terms of an application taking advantage of a smart card's increased data storage, multi-application system environments are excellent examples. Using a contactless smart card, the Transcard program in Sydney, Australia, integrates public transport, retail and banking applications in an open-system environment. While two individual RF/ID and magnetic stripe systems might have served the project requirements, such investment expenditures could not have been shared among the various service providers. The contactless smart card represented a single-time technology investment.

Elvis or the smart card?

The bottom line is that, as selling prices of smart cards decline further and faster than other Auto. ID technologies, the technology moves from just being commercially viable to being a commercial bargain in terms of price and performance. Smart cards offer a business case that is hard to ignore. As increasing numbers of businesses implement them in the next two to three years, you will be more likely to see a smart card in use than Elvis alive at Comdex.

For more information, circle Reader Inquiry Card

Frost & Sullivan

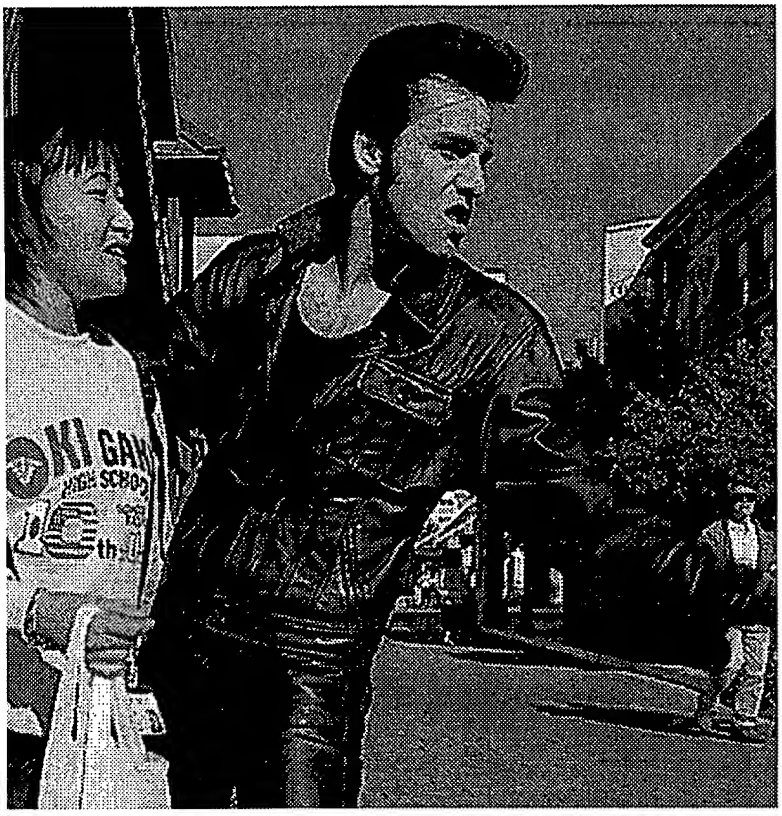
CIRCLE 134

~~~~~~~~

BY ALYXIA DO, GUEST CONTRIBUTOR
~~~~~~~~

Alyxia Do is a research analyst with Frost & Sullivan specializing in the chip and other high-power electronic device markets. She is the lead researcher and author of a strategic research report on world smart card markets that Frost & Sullivan released in February. Do is chairperson for the 1997 Frost & Sullivan Smart Cards Conference on Smart Card Security Systems.

Source: Automatic I.D. News, May97, Vol. 13 Issue 6, pS.20, 2p
Item: 9709031038



What do smart cards and Elvis have in common? Everyone keeps saying they're here, but have you seen either one?? That will change as the prices of smart cards continue to tumble and their security is seen.

Organization TC2100 Bldg./Room PK2

U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

AN EQUAL OPPORTUNITY EMPLOYER